iPhone OS

エンタープライズ配備ガイド

第 2 版（バージョン 3.2 以降）

Apple
1 Infinite Loop
Cupertino, CA 95014
U.S.A.
www.apple.com

アップルジャパン株式会社
〒 163-1480 東京都新宿区西新宿 3 丁目 20 番 2 号
東京オペラシティタワー
www.apple.com/jp

J019-1835/2010-04

目次

iPhone とエンタープライズ

iPhone、iPod touch、および iPad をエンタープライズシステムに統合する方法について説明します。

このガイドはシステム管理者用です。iPhone、iPod touch、および iPad をエンタープライズ環境内で配備およびサポートする方法について説明します。

iPhone OS 3.0 以降のエンタープライズ対応の新機能

iPhone OS 3.x には多数の改良点があり、それにはエンタープライズユーザが特別な関心を持っている以下の項目が含まれます：

- CalDAV カレンダーのワイヤレス同期に対応しています。
- LDAP サーバは、メール、アドレスブック、および SMS の連絡先の検索に対応しています。
- 構成プロファイルは、削除には管理パスワードが必要になるように、暗号化してデバイスにロックすることができます。
- 「iPhone 構成ユーティリティ」で、暗号化された構成プロファイルを、コンピュータに USB で接続されているデバイスに直接追加したり削除したりできます。
- OCSP（オンライン証明書状況プロトコル）が証明書失効に対応しています。
- オンデマンドの証明書ベースの VPN 接続に対応するようになりました。
- 構成プロファイルおよび VPN サーバによる VPN プロキシ構成に対応するようになりました。
- Microsoft Exchange ユーザは、ほかのユーザに会議の参加を依頼できます。Microsoft Exchange 2007 ユーザは、返信状況を表示することもできます。
- Exchange ActiveSync クライアントの証明書ベースの認証に対応しています。
- EAS protocol 12.1 に加え、その他の EAS ポリシーにも対応しています。
- デバイスがロックされるまでの時間を指定したり、カメラを無効にしたり、ユーザがデバイスのディスプレイのスクリーンショットを撮ることを禁止したりなどのデバイス制限を追加できます。
- ローカル・メール・メッセージとカレンダーのイベントを検索することができます。IMAP、MobileMe、および Exchange 2007 の場合は、サーバ上にあるメールも検索できます。
- プッシュメール配信用に追加のメールフォルダを指定できます。
- 構成プロファイルを使用して APN プロキシ設定を指定できます。
- 構成プロファイルを使用して Web クリップをインストールできます。

- 802.1x EAP-SIM に対応するようになりました。
- SCEP（Simple Certificate Enrollment Protocol）サーバを使用して、デバイスを無線で認証して登録できます。
- 「iTunes」でデバイスのバックアップを暗号化されたフォーマットで保存できます。
- 「iPhone 構成ユーティリティ」でスクリプトを使ってプロファイルを作成できます。
- iPhone 構成ユーティリティ 2.2 は、iPad、iPhone、および iPod touch に対応しています。Mac OS X v10.6 Snow Leopard が必要です。Windows 7 にも対応しています。

システム要件

ここでは、システム要件の概要と、iPhone、iPod touch、および iPad をエンタープライズシステムに統合するために利用できるさまざまなコンポーネントの概要について説明します。

iPhone と iPod touch

iPhone および iPod touch デバイスをエンタープライズネットワークで使用するときは、iPhone OS 3.1.x にアップデートする必要があります。

iPad

iPad は、iPhone OS 3.2.x にアップデートする必要があります。

iTunes

デバイスを設定するには、iTunes 9.1 以降が必要です。「iTunes」は、iPhone、iPod touch、および iPad のソフトウェア・アップデートをインストールするためにも必要です。アプリケーションをインストールしたり、音楽、ビデオ、メモ、またはその他のデータを Mac または PC と同期したりするときにも、「iTunes」を使用します。

「iTunes」を使用するには、USB 2.0 ポートが装備された、「iTunes」の Web サイトにリストされている最小要件を満たす Mac または PC が必要です。www.apple.com/jp/itunes/download/ を参照してください。

iPhone 構成ユーティリティ

「iPhone 構成ユーティリティ」では、構成プロファイルの作成、暗号化、およびインストール、プロビジョニングプロファイルと承認されたアプリケーションの追跡とインストール、コンソールログなどのデバイス情報の取得を行うことができます。

「iPhone 構成ユーティリティ」は次のいずれかの要件を満たす必要があります：

- Mac OS X v10.5 Snow Leopard
- Windows XP Service Pack 3（.NET Framework 3.5 Service Pack 1 が必要）
- Windows Vista Service Pack 1（.NET Framework 3.5 Service Pack 1 が必要）
- Windows 7（.NET Framework 3.5 Service Pack 1 が必要）

「iPhone 構成ユーティリティ」は、64 ビットバージョンの Windows 上で、32 ビットモードで動作します。

.Net Framework 3.5 Service Pack 1 のインストーラは、
http://www.microsoft.com/downloads/details.aspx?familyid=ab99342f-5d1a-413d-8319-81da479ab0d7 からダウンロードできます。

このユーティリティにより、構成プロファイルを含む Outlook メッセージを添付ファイルとして作成することができます。さらに、デスクトップのアドレスブックのユーザの名前とメールアドレスを、このユーティリティに接続したデバイスに割り当てることができます。これらの機能は両方とも Outlook を必要とし、Outlook Express と互換性はありません。Windows XP コンピュータでこれらの機能を使用するときは、2007 Microsoft Office System Update のインストールが必要になる場合があります：再配布可能なプライマリ相互運用機能アセンブリ。これは、.NET Framework 3.5 Service Pack 1 より前に Outlook をインストールした場合に必要です。

プライマリ相互運用機能アセンブリのインストーラは、
http://www.microsoft.com/downloads/details.aspx?FamilyID=59daebaa-bed4-4282-a28c-b864d8bfa513 から入手できます。

Microsoft Exchange ActiveSync

iPhone、iPod touch、および iPad は、以下のバージョンの Microsoft Exchange に対応しています：

- Exchange Server 2003 Service Pack 2 用の Exchange ActiveSync（EAS）
- Exchange ActiveSync for Exchange Server（EAS）2007

Exchange 2007 のポリシーと機能のサポートには、Service Pack 1 が必要です。

対応している Exchange ActiveSync ポリシー

次の Exchange ポリシーに対応しています：

- デバイスを使用するためのパスワードを要求（SP2）、パスワードを要求（SP1）
- 最低限必要なパスワードの長さ（文字数）を指定する（SP2）、最低限必要なパスワードの長さ（SP1）
- 次の回数、試行に失敗したらデバイスを無効にする（SP2）、パスワードの入力ミスが許される回数（SP1）
- PIN には数字と文字の両方を含める必要がある（SP2）、英数字のパスワードが必要（SP1）
- 休止時間（分）を指定する（SP2）、ユーザが最後にパスワードを入力してから再入力するまでの時間（分）（SP1）

以下の Exchange 2007 ポリシーにも対応しています：

- 簡易パスワードの許可または禁止
- パスワードの有効期限
- パスワード履歴
- ポリシーの更新間隔
- パスワード内の複合文字の最小数
- ローミング中に手動同期が必要

- カメラを許可
- デバイスの暗号化が必要

各ポリシーの説明については、Exchange ActiveSync の製品ドキュメントを参照してください。

デバイスの暗号化を要求する Exchange ポリシー（RequireDeviceEncryption）は、iPhone 3GS、iPod touch（32 GB 以上の 2009 年秋モデル）、および iPad でサポートされています。iPhone、iPhone 3G、およびその他の iPod touch モデルではデバイスの暗号化がサポートされないため、デバイスの暗号化が必要な Exchange Server には接続できません。

Exchange 2003 で「PIN には数字と文字の両方を含める必要がある」ポリシーを有効にするか、または Exchange 2007 で「英数字のパスワードが必要」ポリシーを有効にすると、ユーザは 1 文字以上の複合文字を含むデバイスパスコードを入力する必要があります。

非アクティブ時間ポリシー（MaxInactivityTimeDeviceLock または AEFrequencyValue）で指定する値は、ユーザが「設定」＞「一般」＞「自動ロック」および「設定」＞「一般」＞「パスコードロック」＞「パスコードを要求」で選択できる最大値を設定するために使用されます。

リモートワイプ

iPhone、iPod touch、または iPad のコンテンツをリモートワイプできます。ワイプによって、デバイス上のすべてのデータと構成情報が取り除かれます。デバイスは安全に消去され、元の出荷時の設定に復元されます。

重要：ワイプによって iPhone および iPhone 3G 上のデータが上書きされます。これには 8 GB のデバイス容量ごとに約 1 時間かかることがあります。ワイプの前にデバイスを電源コンセントに接続してください。電力不足のためにデバイスの電源が切れた場合は、デバイスを電源に接続したときにワイプ処理が再開されます。iPhone 3GS および iPad のワイプによって、データへの暗号化鍵が解除されます（256 ビット AES 暗号化を使って暗号化されています）。ワイプは即座に実行されます。

Exchange Server 2007では、Exchange管理コンソール、Outlook Web Access、またはExchange ActiveSync Mobile Administration Web ツールを使用してリモートワイプを開始できます。

Exchange Server 2003 では、Exchange ActiveSync Mobile Administration Web ツールを使用してリモートワイプを開始できます。

「一般」設定の「リセット」メニューから「すべてのコンテンツと設定を消去」を選択すれば、ユーザが自分のデバイスをワイプすることもできます。パスコードに何回か失敗すると自動的にワイプが開始されるようにデバイスを構成することもできます。

紛失したためにワイプしたデバイスを回復するときは、「iTunes」内のデバイスの最新のバックアップを使って復元します。

Microsoft ダイレクトプッシュ

Exchange サーバは、パケット接続や Wi-Fi データ接続を使用できる場合は、メール、連絡先、カレンダーのイベントを自動的に iPhone および iPad Wi-Fi + 3G に配信します。iPod touch と iPad Wi-Fi にはパケット接続がないため、デバイスが動作中で Wi-Fi ネットワークに接続されているときだけプッシュ通知を受け取ります。

Microsoft Exchange Autodiscovery

Exchange Server 2007 の自動検出サービスに対応しています。デバイスを手動で構成するときは、自動検出によって、メールアドレスとパスワードに基づいて正しい Exchange サーバ情報が自動的に判別されます。自動検出サービスを有効にする方法については、http://technet.microsoft.com/en-us/library/cc539114.aspx を参照してください。

Microsoft Exchange グローバルアドレス一覧

iPhone、iPod touch、および iPad では、Exchange サーバの会社のディレクトリから連絡先情報が取得されます。「連絡先」で検索するときにこのディレクトリにアクセスできます。メールアドレスを入力するときは、このディレクトリが自動的にアクセスされて入力が補完されます。

対応しているその他の Exchange ActiveSync 機能

iPhone OS は、すでに説明した機能に加え、以下の機能に対応しています：

- カレンダーの参加依頼を作成する。Microsoft Exchange 2007 では、参加依頼に対する返信状況を表示することもできます。
- カレンダーのイベントに「予定なし」、「予定あり」、「仮承諾」、または「不在」の状況を設定する。
- サーバ上のメールメッセージを検索する。Microsoft Exchange 2007 が必要です。
- Exchange ActiveSync クライアントの証明書ベースの認証。

対応していない Exchange ActiveSync 機能

対応していない Exchange 機能もあります。例を示します：

- フォルダ管理
- Sharepoint Server に保存された書類へのリンクをメール内で開くこと
- タスクの同期
- 「不在時」の自動応答メッセージを設定すること
- メッセージにフォローアップ用のフラグを設定すること

VPN

iPhone OS は、以下のプロトコルおよび認証方法に対応する VPN サーバに接続できます：

- L2TP/IPSec。MS-CHAPV2 パスワード、RSA SecurID、および CryptoCard によるユーザ認証、および共有シークレットによるコンピュータ認証。
- PPTP。MS-CHAPV2 パスワード、RSA SecurID、および CryptoCard によるユーザ認証。
- Cisco IPSec（パスワード、RSA SecurID、または CryptoCard によるユーザ認証、および共有シークレットと証明書によるコンピュータ認証）。互換性のある Cisco VPN サーバと推奨構成については、「付録 A」を参照してください。

証明書ベースの認証を備えた Cisco IPSec は、構成時に指定するドメインのオンデマンド VPN に対応します。詳しくは、35 ページの「VPN 設定」を参照してください。

ネットワークセキュリティ

iPhone OS は、Wi-Fi Alliance が定義する以下の 802.11i ワイヤレス・ネットワーク・セキュリティ標準に対応しています：

- WEP
- WPA パーソナル
- WPA エンタープライズ
- WPA2 パーソナル
- WPA2 エンタープライズ

また、WPA エンタープライズおよび WPA2 エンタープライズネットワークの以下の 802.1X 認証方法にも対応しています：

- EAP-TLS
- EAP -TTLS
- EAP-FAST
- EAP-SIM
- PEAP v0、PEAP v1
- LEAP

証明書と固有名

iPhone、iPod touch、および iPad では、RSA キーによる X.509 証明書を使用できます。認識されるファイル拡張子は、.cer、.crt、および .der です。証明書チェーンの評価は、「Safari」、「メール」、「VPN」、およびその他のアプリケーションによって実行されます。

固有名が 1 つだけ含まれる P12（PKCS #12 標準）ファイルを使用します。認識されるファイル拡張子は、.p12 および .pfx です。固有名がインストールされると、ユーザはそれを保護しているパスフレーズの入力を求められます。

信頼されるルート証明書への証明書チェーンを確立するために必要な証明書は、手動でまたは構成プロファイルを使ってインストールできます。デバイス上にあらかじめ用意されているルート証明書は追加する必要はありません。インストール済みのシステムルートのリストについては、アップルのサポート記事（英語版）（http://support.apple.com/kb/HT3580）を参照してください。

証明書は、SCEP 経由で安全に無線でインストールできます。詳しくは、22 ページの「認証されている登録および構成プロセスの概要」を参照してください。

メールアカウント

iPhone、iPod touch、および iPad は、Windows、UNIX、Linux、Mac OS X などのさまざまなサーバプラットフォーム上で、業界標準の IMAP4 および POP3 対応のメールソリューションに対応しています。IMAP を使って Exchange アカウントからメールにアクセスしたり、ダイレクトプッシュが有効になっている Exchange アカウントを使用することもできます。

ユーザが自分のメールを検索する場合は、検索をメールサーバで続行するオプションがあります。これは、Microsoft Exchange Server 2007 と、大半の IMAP ベースのアカウントで使用できます。

Exchange のユーザ ID とパスワードなどのユーザのメールアカウント情報は、デバイス上にセキュリティ保護された状態で保存されます。

LDAP サーバ

iPhone、iPod touch、および iPad では、会社の LDAPv3 サーバ上の会社のディレクトリから連絡先情報が取得されます。「連絡先」で検索するときにこれらのディレクトリにアクセスできます。また、メールアドレスを入力するときは、このディレクトリが自動的にアクセスされてメールアドレスが補完されます。

CalDAV サーバ

iPhone、iPod touch、および iPad では、カレンダーデータが会社の CalDAV サーバと同期されます。カレンダーに対する変更は、デバイスとサーバ間で定期的にアップデートされます。

また、休日のカレンダーや同僚のスケジュールのカレンダーなど、読み取り専用の公開されたカレンダーを照会することもできます。

デバイスからの新しいカレンダーの参加依頼の作成と送信は、CalDAV アカウントでは対応していません。

その他の参考資料

このガイド以外に、以下の出版物や Web サイトで役に立つ情報が提供されています：

- 「iPhone とエンタープライズ」の Web ページ（www.apple.com/jp/iphone/enterprise/）
- 「ビジネスに iPad を」の Web ページ （www.apple.com/jp/ipad/business/）
- Exchange 製品の概要（http://technet.microsoft.com/en-us/library/bb124558.aspx）
- Exchange ActiveSync の配備 (http://technet.microsoft.com/en-us/library/aa995962.aspx)
- Exchange 2003 テクニカルライブラリ（http://technet.microsoft.com/en-us/library/bb123872(EXCHG.65).aspx）
- Exchange ActiveSync セキュリティの管理（http://technet.microsoft.com/en-us/library/bb232020(EXCHG.80).aspx）
- 「Wi-Fi for Enterprise」の Web ページ（www.wi-fi.org/enterprise.php）
- iPhone VPN と Cisco Adaptive Security Appliances（ASA）との接続（www.cisco.com/en/US/docs/security/vpn_client/cisco_vpn_client/iPhone/2.0/connectivity/guide/iphone.html）
- 「iPhone ユーザガイド」(www.apple.com/jp/support/iphone/ からダウンロードできます)。iPhone 上でこのユーザガイドを表示するには、「Safari」で「iPhone ユーザガイド」のブックマークをタップするか、http://help.apple.com/iphone/ にアクセスしてください。
- iPhone のビデオガイド（www.apple.com/jp/iphone/guidedtour/）
- 「iPod touch ユーザガイド」(www.apple.com/jp/support/ipodtouch からダウンロードできます)。iPod touch でこのユーザガイドを表示するには、「Safari」で「iPod touch ユーザガイド」をタップするか、http://help.apple.com/ipodtouch/ にアクセスしてください。
- iPod touch のビデオガイド（www.apple.com/jp/ipodtouch/guidedtour/）
- 「iPad ユーザガイド」（www.apple.com/jp/support/ipad からダウンロードできます）。iPad 上でこのユーザガイドを表示するには、「Safari」で「iPad ユーザガイド」をタップするか、http://help.apple.com/ipad/ にアクセスしてください。
- iPad のビデオガイド（www.apple.com/ipad/guided-tour/）

iPhone および iPod touch を配備する 1

この章では、iPhone、iPod touch、および iPad をエンタープライズ内に配備する方法の概要を説明します。

iPhone、iPod touch、および iPad は、Microsoft Exchange 2003 および 2007、802.1X ベースのセキュリティ保護されたワイヤレスネットワーク、および Cisco IPSec 仮想プライベートネットワークなど、エンタープライズシステムに簡単に統合できるように設計されています。あらゆるエンタープライズソリューションと同様に、配備オプションを適切に計画して理解することで、配備をより簡単に効率的に行うことができます。

iPhone、iPod touch、および iPad の配備を計画するときは、次の点を考慮してください：

- 会社の iPhone と iPad（Wi-Fi + 3G モデル）をワイヤレスパケット通信サービスにどのようにアクティベーションしますか？
- ユーザはどのエンタープライズ・ネットワーク・サービス、アプリケーション、およびデータにアクセスする必要がありますか？
- 会社の機密データを保護するためにどのようなポリシーをデバイスに設定したいですか？
- デバイスを個別に手動で構成したいですか、または効率的な方法を使って多数のデバイスを構成したいですか？

エンタープライズ環境、IT ポリシー、ワイヤレスキャリア、およびコンピュータと通信の要件によって、配備戦略の調整方法が異なってきます。

デバイスをアクティベーションする

iPhone を使って電話をかけたり、電話に出たり、テキストメッセージを送信したり、パケット通信に接続するには、iPhone がワイヤレスキャリアにアクティベーションされている必要があります。個人および法人の音声通話料金、データ通話料金、およびアクティベーション手順については、キャリアに問い合わせてください。

iPhone には SIM カードを取り付ける必要があります。SIM カードを取り付けた後に、「iTunes」を使って iPhone をコンピュータに接続してアクティベーション処理を完了する必要があります。SIM カードがすでに有効になっている場合は、iPhone がすぐに使用できる状態です。そうでない場合は、「iTunes」の指示に従って新しいサービスのアクティベーション処理を行ってください。

iPad をアクティベーションするには、「iTunes」を使って iPad がコンピュータに接続されている必要があります。米国内の iPad Wi-Fi + 3G の場合は、iPad を使って AT&T のデータプランにサインアップして管理（またはキャンセル）します。「設定」＞「パケット接続」＞「アカウントを表示」と移動します。iPad のロックが解除されるので、好きなキャリアを使用できます。アカウントを設定して互換性のあるマイクロ SIM カードを入手する場合は、キャリアに問い合わせてください。米国では、AT&T と互換性のあるマイクロ SIM カードが iPad Wi-Fi + 3G に付属しています。

iPod touch および iPad Wi-Fi 用のパケット通信サービスや SIM カードはありませんが、アクティベーションのために「iTunes」を使って同様にコンピュータに接続する必要があります。

アクティベーション処理を完了するには「iTunes」が必要なので、「iTunes」を各ユーザの Mac または PC にインストールするかどうか、または各デバイスにインストールされている「iTunes」を使ってアクティベーションを完了するかどうかを決定する必要があります。

アクティベーションした後は、エンタープライズシステムでデバイスを使用するために「iTunes」は必要ありませんが、ミュージック、ビデオ、および Web ブラウザのブックマークをコンピュータと同期するときには必要になります。また、デバイスにソフトウェア・アップデートをダウンロードしてインストールするときや、エンタープライズアプリケーションをインストールするときにも必要になります。

デバイスのアクティベーションと「iTunes」の使いかたについて詳しくは、第 4 章を参照してください。

ネットワークサービスとエンタープライズデータへのアクセスを準備する

iPhone OS 3.x ソフトウェアでは、既存の Microsoft Exchange Server 2003 または 2007 ソリューションを使って、メール、連絡先、およびカレンダーを安全にプッシュしたり、アドレスをグローバル参照したり、リモートワイプしたり、デバイスにパスコードポリシーを適用したりできます。また、会社のリソースに安全に接続するときにも、802.1X ワイヤレス認証を使用して WPA エンタープライズおよび WPA2 エンタープライズワイヤレスネットワーク経由でアクセスするか、または PPTP、LT2P over IPSec、または Cisco IPSec プロトコルを使用して VPN 経由でアクセスするか、あるいはその両方を利用してアクセスすれば、安全に接続することができます。

会社で Microsoft Exchange が使用されていない場合でも、iPhone または iPod touch のメールを標準的な POP または IMAP ベースのサーバやサービスとワイヤレスで同期することができます。また、「iTunes」を使用して、Mac OS X の「iCal」や「アドレスブック」または Windows PC 上の「Microsoft Outlook」からカレンダーイベントと連絡先を同期することもできます。カレンダーとディレクトリへのワイヤレスアクセスについては、CalDAV と LDAP が対応しています。

ユーザがアクセスするネットワークサービスを決定するときは、これ以降のセクションの情報を参照してください。

Microsoft Exchange

iPhone は、Microsoft Exchange ActiveSync（EAS）経由で Microsoft Exchange Server に直接接続します。Exchange ActiveSync は、新しいメールメッセージや会議の参加依頼が届いたらデバイスがすぐにアップデートされるように、Exchange Server と iPhone または iPad Wi-Fi + 3G との間の接続を監視しています。iPod touch と iPad Wi-Fi にはパケット接続がないので、デバイスが動作中で Wi-Fi ネットワークに接続されているときにだけプッシュ通知を受け取ります。

会社の Exchange Server 2003 または Exchange Server 2007 上で Exchange ActiveSync に現在対応している場合は、すでに必要なサービスが適切に構成されています。Exchange Server 2007 の場合は、「クライアントアクセスの役割」がインストールされていることを確認してください。Exchange Server 2003 の場合は、Outlook Mobile Access（OMA）が有効になっていることを確認してください。

会社に Exchange Server は配備されているけれども、Exchange ActiveSync をはじめて使用する場合は、これ以降のセクションの情報を確認してください。

ネットワーク構成

- ファイアウォールでポート 443 が開いていることを確認します。会社で Outlook Web Access が使用されている場合は、ポート 443 がすでに開いている可能性が高いです。
- IIS の Microsoft Server ActiveSync ディレクトリに接続するときに SSL 接続を要求するために、サーバ証明書がフロントエンド Exchange サーバにインストールされ、認証方法のプロパティで基本認証のみが有効になっていることを確認します。

- Microsoft ISA（Internet Security and Acceleration）サーバを使用する場合は、サーバ証明書がインストールされていることを確認してから、着信接続が適切に解決されるようにパブリック DNS をアップデートします。
- ネットワークの DNS からイントラネットおよびインターネットクライアントの Exchange ActiveSync サーバに、外部ルーティング可能な 1 つのアドレスが返されることを確認します。これは、両方の接続が動作中のときに、デバイスがサーバに接続するときに同じ IP アドレスを使用できるようにするために必要です。
- Microsoft ISA サーバを使用する場合は、Web リスナーと Exchange Web クライアントアクセス公開ルールを作成します。詳細は、Microsoft の製品ドキュメントを参照してください。
- すべてのファイアウォールとネットワークアプライアンスのアイドル・セッション・タイムアウトを 30 分に設定します。ハートビートおよびタイムアウトの間隔については、Microsoft Exchange の製品ドキュメント（http://technet.microsoft.com/en-us/library/cc182270.aspx）を参照してください。

Exchange アカウント設定

- Active Directory サービスを使用するユーザまたはグループのために、Exchange ActiveSync を有効にします。Exchange Server 2003 および Exchange Server 2007 の組織レベルでは、これらはすべてのモバイルデバイスについてデフォルトで有効になっています。Exchange Server 2007 の場合は、Exchange 管理コンソールの「受信者の構成」を確認してください。
- Exchange システムマネージャを使用してモバイル機能、ポリシー、およびデバイスセキュリティ設定を構成します。Exchange Server 2007 の場合は、Exchange 管理コンソールで行います。
- Microsoft Exchange ActiveSync Mobile Administration Web ツールをダウンロードしてインストールします。リモートワイプを開始するために必要です。Exchange Server 2007 の場合は、Outlook Web Access または Exchange 管理コンソールを使用してリモートワイプを開始することもできます。

WPA/WPA2 エンタープライズ Wi-Fi ネットワーク

WPA エンタープライズと WPA2 エンタープライズに対応することで、iPhone、iPod touch、および iPad から会社のワイヤレスネットワークに安全にアクセスできるようになります。WPA/WPA2 エンタープライズでは AES 128 ビット暗号化が使用されます。これは実績のあるブロックベースの暗号化方式で、会社のデータが高いレベルで継続的に保護されます。

802.1X 認証に対応することで、iPhone OS デバイスをさまざまな RADIUS サーバ環境に統合することができます。802.1X ワイヤレス認証方式に対応しているので、EAP-TLS、EAP-TTLS、EAP-FAST、PEAPv0、PEAPv1、および LEAP を利用できます。

WPA/WPA2 エンタープライズネットワーク構成

- ネットワークアプライアンスの互換性を確認し、iPhone、iPod touch、および iPad が対応している認証タイプ（EAP タイプ）を選択します。認証サーバ上で 802.1X が有効になっていることを確認します。さらに必要に応じて、サーバ証明書をインストールし、ユーザとグループにネットワークアクセス権を割り当てます。

- 802.1X 認証用のワイヤレス・アクセス・ポイントを構成し、対応する RADIUS サーバ情報を入力します。
- RADIUS認証が適切に構成されていることを確認するために、MacまたはPCで802.1Xの配備をテストします。
- 証明書ベースの認証を使用することを計画している場合は、公開鍵インフラストラクチャがその鍵配布プロセスでデバイスおよびユーザベースの証明書をサポートするように構成されていることを確認します。
- 証明書フォーマットとデバイスおよび認証サーバとの互換性を確認します。証明書については、11 ページの「証明書と固有名」を参照してください。

仮想プライベートネットワーク

iPhone、iPod touch、および iPad では、プライベートネットワークにセキュリティ保護されたアクセスを行うために、Cisco IPSec、L2TP over IPSec、および PPTP 仮想プライベート・ネットワーク・プロトコルが使用されます。組織がこれらのいずれかのプロトコルに対応している場合は、VPN インフラストラクチャでデバイスを使用するために追加のネットワーク構成や他社製アプリケーションは必要ありません。

Cisco IPSec を配備することで、業界標準の x.509 証明書による証明書ベースの認証を利用できるようになります。さらに、証明書ベースの認証により、エンタープライズネットワークへのシームレスでセキュリティ保護されたワイヤレスアクセスを可能にする、VPN オンデマンドを利用できるようになります。

2 要素トークンベース認証のために、iPhone OS は RSA SecurID および CryptoCard に対応しています。ユーザは VPN 接続を確立するときに、自分の PIN およびトークンが生成したワンタイムパスワードをデバイスに直接入力します。互換性のある Cisco VPN サーバと推奨構成については、「付録 A」を参照してください。

iPhone、iPod touch、および iPad は、Cisco IPSec と L2TP/IPSec が配備された環境のための共有シークレット認証、およびユーザ名とパスワードによる基本認証のための MS-CHAPv2 にも対応しています。

VPN プロキシ自動構成（PAC および WPAD）も対応しています。これにより、特定の URL にアクセスするためのプロキシサーバ設定を指定できます。

VPN 設定のガイドライン

- iPhone OS は既存のほとんどの VPN ネットワークと互換性があるので、デバイスからネットワークにアクセスするために必要な構成は最小限で済みます。配備を準備するときは、会社の既存の VPN プロトコルと認証方式に iPhone が対応しているかどうかを確認することをお勧めします。
- VPN コンセントレータの規格と互換性があることを確認します。また、iPhone OS が対応する規格が実装内で有効になっていることを確認するために、RADIUS または認証サーバへの認証パスを確認することもお勧めします。
- お使いのソフトウェアや機器が最新のセキュリティパッチやファームウェアでアップデートされていることを、ソリューションプロバイダに問い合わせて確認してください。

- URL 固有のプロキシ設定を構成したい場合は、PAC ファイルを基本 VPN 設定でアクセスできる Web サーバ上に置いて、MIME タイプ application/x-ns-proxy-autoconfig で使用されるようにします。または、同じようにアクセスできるサーバ上の WPAD ファイルの場所を指定するように、DNS または DHCP を構成します。

IMAP メール

Microsoft Exchange を使用していない場合でも、使用するメールサーバが IMAP をサポートしてユーザ認証と SSL を要求するように構成されていれば、セキュリティ保護された標準ベースのメールソリューションを実装することができます。たとえば、この手法を使って Lotus Notes/Domino または Novell GroupWise のメールにアクセスできます。これらのメールサーバは、DMZ サブネットワークの内部、または会社のファイアウォールの背後、あるいはその両方に配備できます。

SSL が実装されている iPhone OS は、128 ビット暗号化および主要な認証局が発行する X.509 証明書に対応しています。また、業界標準の MD5 チャレンジレスポンスや NTLMv2 などの強力な認証方式にも対応しています。

IMAP ネットワーク設定のガイドライン

- セキュリティ保護を強化する場合は、信頼された認証局（CA）から発効されたデジタル証明書をサーバにインストールしてください。CA からの証明書をインストールすることは、プロキシサーバを会社のインフラストラクチャ内で信頼されたエンティティにするための重要な手順です。証明書を iPhone にインストールする方法については、38 ページの「資格情報の設定」を参照してください。
- iPhone OS デバイスがサーバからメールを取得できるようにするには、ファイアウォールでポート 993 を開き、プロキシサーバが IMAP over SSL に設定されていることを確認します。
- デバイスからメールを送信できるようにするには、ポート 587、465、または 25 が開いている必要があります。ポート 587 が最初に使用されます。このように選択することをお勧めします。

LDAP ディレクトリ

iPhone OS では、標準ベースの LDAP ディレクトリサーバにアクセスすることができ、Microsoft Exchange のグローバルアドレス一覧と同様のグローバル・アドレス・ディレクトリなどの情報を提供することができます。

デバイスで LDAP アカウントが構成されていると、デフォルトの検索ベースを識別するため、サーバのルートレベルで属性 `namingContexts` が検索されます。検索範囲はデフォルトではサブツリーに設定されています。

CalDAV カレンダー

iPhone OS の CalDAV のサポートにより、Microsoft Exchange を使用していない組織へのグローバルカレンダーとスケジュールが提供されます。iPhone OS は CalDAV 標準に対応するカレンダーサーバと連動します。

照会するカレンダー

休日や特別なイベントスケジュールなど、会社のイベントの読み取り専用のカレンダーを公開したい場合は、iPhone OS デバイスでカレンダーを照会し、Microsoft Exchange および CalDAV のカレンダーと一緒に情報を表示することができます。iPhone OS では標準の iCalendar（.ics）フォーマットのカレンダーファイルを使用します。

照会するカレンダーをユーザに配信するときは、SMS またはメールで完全修飾 URL を送信するのが簡単です。ユーザがリンクをタップすると、指定されたカレンダーが照会されます。

エンタープライズアプリケーション

iPhone OSのエンタープライズアプリケーションを配備するには、「iPhone構成ユーティリティ」または「iTunes」を使用して、それらのアプリケーションをデバイスにインストールしてください。アプリケーションをユーザのデバイスに配備した後は、ユーザの Mac または PC に「iTunes」がインストールされていれば、それらのアプリケーションをより簡単にアップデートできます。

オンライン証明書状況プロトコル

iPhone OS デバイス用のデジタル証明書を提供するときは、OCSP 対応の証明書を発行することを考慮してください。こうすることで、デバイスは証明書が失効していないかどうかを OCSP サーバに確認してから使用できます。

デバイスのパスコードポリシーを決定する

ユーザがアクセスするネットワークサービスとデータを決定した後に、実装したいデバイス・パスコード・ポリシーを決定する必要があります。

会社のネットワーク、システム、またはアプリケーションがパスワードや認証トークンを要求しない場合は、デバイス上でパスコードを要求するように設定することをお勧めします。802.1X ネットワークまたは Cisco IPSec VPN で証明書ベースの認証を使用する場合、またはログイン資格情報を保存するエンタープライズアプリケーションの場合は、デバイスパスコードを設定しそのタイムアウトを短く設定するようユーザに要求することをお勧めします。デバイスが紛失したり盗まれても、デバイスパスコードを知らない限り使用できないようにするためです。

ポリシーを iPhone、iPod touch、および iPad に設定する方法は 2 つあります。デバイスが Microsoft Exchange アカウントにアクセスするように構成されている場合は、Exchange ActiveSync ポリシーがデバイスにワイヤレスでプッシュされます。これにより、ユーザが何もしなくても、ポリシーを適用してアップデートすることができます。EAS ポリシーについては、8 ページの「対応している Exchange ActiveSync ポリシー」を参照してください。

Microsoft Exchange を使用しない場合は、構成プロファイルを作成することによって、同様のポリシーをデバイスに設定できます。ポリシーを変更したい場合は、アップデートしたプロファイルをユーザに投稿または送信するか、「iPhone 構成ユーティリティ」を使用してプロファイルをインストールする必要があります。デバイス・パスコード・ポリシーについては、32 ページの「パスコード設定」を参照してください。

Microsoft Exchange を使用する場合は、構成ポリシーを使用することで、EAS ポリシーを補完することもできます。こうすることで、Microsoft Exchange 2003 で利用できないポリシーにアクセスしたり、iPhone OS デバイス専用のポリシーを定義したりできます。

デバイスを構成する

各 iPhone、iPod touch、および iPad をどのように構成するかを決定する必要があります。これは、今後どのくらいの数のデバイスを配備および管理する予定なのかによってある程度左右されます。数が少ない場合は、デバイスを自分で手動で構成する方が簡単な場合があります。その場合、デバイスを使って、各メールアカウントの設定、Wi-Fi 設定、および VPN 構成情報を入力する必要があります。手動構成について詳しくは、第 3 章を参照してください。

多数のデバイスを配備する場合や、メール設定、ネットワーク設定、およびインストールする証明書が大量にある場合は、構成プロファイルを作成して配信することによってデバイスを構成することをお勧めします。構成プロファイルを使用すれば、設定と認証情報がデバイスにすぐに読み込まれます。一部の VPN および Wi-Fi 設定は、構成プロファイルを使用しなければ設定できません。Microsoft Exchange を使用しない場合は、構成プロファイルを使用してデバイス・パスコード・ポリシーを設定する必要があります。

構成プロファイルは暗号化して署名することができ、これにより特定のデバイス以外での使用を制限したり、プロファイルに含まれている設定を他の人が変更できないようにすることができます。また、プロファイルに対してデバイスにロックされているというマークを付けて、インストール後は、すべてのデータのデバイスをワイプせずに（または、オプションで管理パスワードを使って）削除することはできないようにすることができます。

デバイスを手動で構成する場合も、構成プロファイルを使用する場合も、自分でデバイスを構成するのかまたはこの作業をユーザに委任するのかどうかも決定する必要があります。どちらを選択するかは、ユーザの場所、ユーザが自分の IT 機器を管理できるかどうかに関連する会社の方針、および配備しようとしているデバイス構成の複雑さによって決まります。構成プロファイルは、大企業、遠隔地の従業員、または自分のデバイスを設定できないユーザに適しています。

ユーザに自分でデバイスをアクティベーションしてほしい場合や、ユーザがエンタープライズアプリケーションをインストールまたはアップデートする必要がある場合は、各ユーザの Mac または PC に「iTunes」がインストールされている必要があります。「iTunes」は、iPhone OS のソフトウェア・アップデートを実行するときにも必要になります。このため、ユーザに「iTunes」を配信しないことを決定した場合は、その点を忘れないようにしてください。「iTunes」の配備については、第 4 章を参照してください。

無線での登録と構成

登録とは、証明書の配信プロセスを自動化できるように、デバイスとユーザを認証するプロセスのことです。デジタル証明書には、ユーザに多くの利点があります。デジタル証明書を使用して、Microsoft Exchange ActiveSync、WPA2 エンタープライズワイヤレスネットワーク、会社の VPN 接続などの重要なエンタープライズサービスへのアクセスを認証することができます。証明書ベースの認証により、会社のネットワークにシームレスにアクセスするための VPN オンデマンドの使用も許可されます。

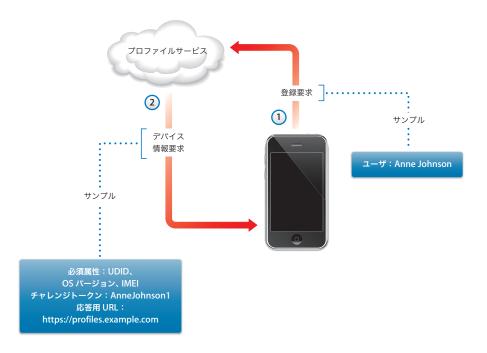
無線登録機能を使用して会社の PKI（公開鍵インフラストラクチャ）の証明書を発行するほか、デバイス構成プロファイルを配備することもできます。これにより確実に、会社のサービスに信頼されたユーザのみがアクセスすることでき、そのデバイスが IT ポリシーに従って構成されることになります。また、構成プロファイルは暗号化もロックもできるため、設定の削除や変更はできず、ほかのユーザと共有することはできません。これらの機能は、以下で説明する無線プロセスで使用できます。また、管理コンピュータに接続されているときに、「iPhone 構成ユーティリティ」を使用してデバイスを構成することによって使用することもできます。「iPhone 構成ユーティリティ」の使いかたについては、第 2 章を参照してください。

無線での登録と構成の実装には、認証、ディレクトリ、および証明書サービスの開発と統合が必要です。このプロセスは標準の Web サービスを使用して配備することができ、適切な場所に配備した後、ユーザが安全で認証された方法でデバイスを設定できるようになります。

認証されている登録および構成プロセスの概要

このプロセスを実装するには、HTTP 接続の許可、ユーザの認証、mobileconfig プロファイルの作成、およびこのセクションで説明するプロセス全体の管理を行う、独自のプロファイル配信サービスを作成する必要があります。

SCEP（Simple Certificate Enrollment Protocol）を使用してデバイス資格情報を発行するには、CA（認証局）も必要です。PKI、SCEP、および関連トピックへのリンクについては、27 ページの「その他の参考資料」を参照してください。

次の図は、iPhone が対応している登録と構成のプロセスを示しています。

フェーズ 1 - 登録を始める

フェーズ 1 – 登録を始める： 登録は、ユーザが「Safari」を使用して、作成したプロファイル配信サービスの URL にアクセスすることから始まります。この URL を SMS またはメールで配信できます。図の手順 1 として示される登録要求は、ユーザの固有名を認証する必要があります。認証を基本認証のようにシンプルにしたり、既存のディレクトリサービスに組み込むことができます。

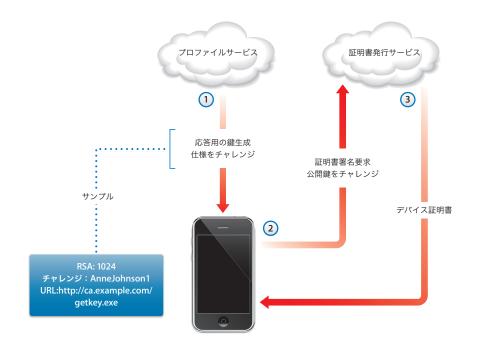
手順 2 では、サービスが応答して構成プロファイル（.mobileconfig）を送信します。この応答では、構成プロセスをユーザごとにカスタマイズできるように、デバイスが次の返信で提供する必要のある属性のリストと、このプロセスの間ユーザの固有名を繰り越すことができるにする事前共有キー（チャレンジ）を指定します。サービスが要求できるデバイス属性は、iPhone OS バージョン、デバイス ID（MAC アドレス）、プロダクトタイプ（iPhone 3GS は iPhone2,1 を返します）、IMEI（携帯電話 ID）、および ICCID（SIM 情報）です。

このフェーズの構成プロファイルのサンプルについては、83 ページの「フェーズ 1 – サーバ応答のサンプル」を参照してください。

フェーズ 2 - デバイスの認証

フェーズ 2 – デバイスの認証： ユーザがフェーズ 1 で受信したプロファイルのインストールを受け入れた後、デバイスは要求された属性を検索し、チャレンジ応答（指定されている場合）を追加し、組み込みの固有名（アップル発行の証明書）を使用して応答に署名し、それを HTTP Post を使用してプロファイル配信サービスに返信します。

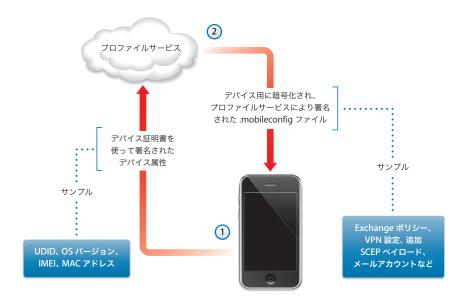
このフェーズの構成プロファイルのサンプルについては、84 ページの「フェーズ 2 - デバイス応答のサンプル」を参照してください。

フェーズ 3 - デバイス証明書のインストール

フェーズ 3 – 証明書のインストール： 手順 1 では、プロファイル配信サービスが、鍵（RSA 1024）を生成するために使用する仕様と、SCEP（Simple Certificate Enrollment Protocol）を使用して証明書用にその鍵を返す場所について応答します。

手順 2 では、SCEP 要求は、要求を認証するために SCEP パケットからチャレンジを使用して、自動モードで処理する必要があります。

手順 3 では、CA がデバイスの暗号化証明書で応答します。

このフェーズのサンプルの構成プロファイルについては、85 ページの「フェーズ 3 - SCEP 仕様によるサーバ応答のサンプル」を参照してください。

フェーズ 4 - デバイスの構成

フェーズ 4 – デバイスの構成： 手順 1 では、デバイスが、前のフェーズで CA から提供された暗号化証明書を使用して署名された、属性のリストを返信します。

手順 2 では、プロファイルサービスは、自動的にインストールされている暗号化された .mobileconfig ファイルで応答します。プロファイルサービスが .mobileconfig ファイルに署名します。たとえば、その SSL 証明書をこの目的のために使用できます。

一般設定に加えて、この構成プロファイルには適用したいエンタープライズポリシーを定義し、ユーザがデバイスから削除できないようにロックされたプロファイルにする必要があります。構成プロファイルには、プロファイルがインストールされるときに実行される、SCEP を使用した固有名の登録の追加要求を含めることができます。

同様に、SCEP を使ってインストールした証明書の有効期限が切れていたり、何らかの理由で無効になっているときは、ユーザはプロファイルのアップデートを求められます。ユーザがその要求を承認すると、デバイスは前述のプロセスを繰り返して新しい証明書とプロファイルを取得します。

このフェーズの構成プロファイルのサンプルについては、86 ページの「フェーズ 4 - デバイス応答のサンプル」を参照してください。

その他の参考資料

- IPSec VPN のデジタル証明書 PKI（https://cisco.hosted.jivesoftware.com/docs/DOC-3592）
- 公開鍵インフラストラクチャ（http://en.wikipedia.org/wiki/Public_key_infrastructure）
- IETF SCEP プロトコル仕様（http://www.ietf.org/internet-drafts/draft-nourse-scep-18.txt）

エンタープライズ内の iPhone、iPod touch、および iPad に関するその他の情報と参考資料は、www.apple.com/jp/iphone/enterprise および www.apple.com/jp/ipad/business で入手できます。

構成プロファイルを作成する／配備する　2

構成プロファイルは、iPhone、iPad、および iPod touch がエンタープライズシステムをどのように利用するかを定義します。

構成プロファイルは XML ファイルであり、iPhone、iPod touch、および iPad でエンタープライズシステムを利用するための、デバイスのセキュリティポリシーと制限、VPN 構成情報、Wi-Fi 設定、メールとカレンダーのアカウント、および認証資格情報が含まれます。

構成プロファイルは、「iPhone 構成ユーティリティ」を使用して USB でコンピュータに接続されているデバイスにインストールできます。または、メールや Web ページを使用して構成プロファイルを配信することもできます。ユーザがそのメールの添付ファイルを開いたり、デバイス上の「Safari」を使ってプロファイルをダウンロードしたりすると、インストール処理を開始することを求められます。

構成プロファイルを作成および配信したくない場合は、デバイスを手動で構成することもできます。詳しくは、第 3 章を参照してください。

iPhone 構成ユーティリティについて

「iPhone 構成ユーティリティ」では、構成プロファイルの作成、暗号化、およびインストール、プロビジョニングプロファイルと承認されたアプリケーションの追跡とインストール、コンソールログなどのデバイス情報の取得を簡単に行うことができます。「iPhone 構成ユーティリティ」のインストーラを実行すると、このユーティリティが、Mac OS X では「/ アプリケーション / ユーティリティ /」に、Windows では「Programs\iPhone Configuration Utility\」にインストールされます。

「iPhone 構成ユーティリティ」を開くと、以下のようなウインドウが表示されます。

このウインドウのほとんどの内容は、サイドバーの項目を選択すると変わります。

サイドバーにはライブラリが表示され、次の項目が表示されます：

- デバイス：コンピュータに接続したことのある iPhone および iPod touch デバイスのリストが表示されます。
- アプリケーション：コンピュータに接続されているデバイスにインストールできるアプリケーションのリストが表示されます。プロビジョニングプロファイルは、アプリケーションをデバイス上で実行するために必要になる場合があります。
- プロビジョニングプロファイル：デバイスのプロファイル（iPhone OS のために開発したものを Apple Developer Connection によって承認された方法で使用することが許可されます）のリストが表示されます。詳しくは、第 5 章を参照してください。プロビジョニングプロファイルにより、デバイスで、iTunes Store では配信されないエンタープライズアプリケーションを実行することもできます。

- **構成プロファイル**：以前に作成した構成プロファイルのリストが表示されます。入力した情報を編集したり、ユーザに送信したり接続されているデバイスにインストールできる新しい構成を作成したりできます。

サイドバーには「**接続済みデバイス**」も表示されます。現在コンピュータの USB ポートに接続されている iPhone OS デバイスに関する情報が表示されます。接続されているデバイスに関する情報はデバイスリストに自動的に追加されるため、デバイスを再接続しなくても何度でも見ることができます。デバイスを接続した後は、そのデバイスのみで使用するプロファイルを暗号化することもできます。

デバイスが接続されている場合は、「iPhone 構成ユーティリティ」を使用して構成プロファイルとアプリケーションをデバイスにインストールできます。詳しくは、40 ページの「iPhone 構成ユーティリティを使用して構成プロファイルをインストールする」、66 ページの「iPhone 構成ユーティリティを使用してアプリケーションをインストールする」、および 65 ページの「iPhone 構成ユーティリティを使用してプロビジョニングプロファイルをインストールする」を参照してください。

デバイスが接続されているときに、コンソールログとクラッシュログ（記録されている場合）も表示することができます。これらのデバイスログは、Mac OS X 上の Xcode 開発環境内で表示できるものと同じログです。

構成プロファイルを作成する

このマニュアルでは、**構成 プロファイル**と**ペイロード**という用語を使用します。構成プロファイルとは、iPhone、iPod touch、または iPad に特定（単一または複数）の設定を構成するファイル全体のことです。ペイロードとは、構成プロファイル内の特定のタイプの設定（VPN 設定など）の個々の集まりのことです。

組織に必要なすべてのペイロードを含む 1 つの構成プロファイルを作成することはできますが、各タイプの情報を別個にアップデートしたり配信できるように、証明書用に 1 つのプロファイルを作成し、その他の設定用に別の 1 つ（または複数）のプロファイルを作成することを検討してください。また、ユーザが VPN またはアカウント設定が含まれる新しいプロファイルをインストールするときに、すでにインストール済みの証明書を残しておくことができます。

多くのペイロードでは、ユーザ名とパスワードを指定できます。この情報を省略した場合は、複数のユーザがプロファイルを使用できますが、プロファイルをインストールするとき、不足している情報の入力が求められます。プロファイルをユーザごとにカスタマイズし、パスワードを含める場合は、内容を保護するためにプロファイルを暗号化されたフォーマットで配信する必要があります。詳しくは、40 ページの「構成プロファイルをインストールする」を参照してください。

新しい構成プロファイルを作成するには、「iPhone 構成ユーティリティ」のメニューバーで、「ファイル」＞「新規構成プロファイル」と選択します。または、ライブラリから「構成プロファイル」を選択し、ツールバーの「新規」ボタンをクリックします。ペイロードのリストを使用して、プロファイルにペイロードを追加します。次に、編集パネルに表示されるオプションを入力したり選択することで、ペイロードを編集します。必須フィールドには赤い矢印が付いています。（iPhone Configuration Web Utility では表示されません。）W-Fi などの一部の設定では、「追加」（＋）ボタンをクリックすることで構成を追加できます。構成を取り除くときは、編集パネルで「削除」（−）ボタンをクリックします。

ペイロードを編集するには、ペイロードのリストで該当する項目を選択し、「構成」ボタンをクリックしてから、以下の説明に従って情報を入力してください。

構成プロファイルの作成を自動化する

AppleScript（Mac 上）または C# スクリプト（Windows 上）を使用することで、構成ファイルの作成を自動化することもできます。対応しているメソッドとその構文を確認するには、次のようにしてください：

- Mac OS X：「スクリプトエディタ」を使って、iPhone 構成ユーティリティ用の AppleScript 用語説明を開きます。
- Windows：Visual Studio を使って、iPCUScripting.dll が提供するメソッド呼び出しを表示します。

スクリプトを実行するには、Mac 上で AppleScript Tell コマンドを使用します。Windows 上では、スクリプト名をコマンド行パラメータとして「iPhone 構成ユーティリティ」に渡します。

例については、付録 C「サンプルスクリプト」を参照してください。

一般設定

ここにはこのプロファイルの名前と識別子を入力し、ユーザがインストール後にプロファイルを削除できるかどうかを指定します。

名前
プロファイルの表示名（デバイス上に表示）
Example Contractor Profile

識別子
プロファイルの一意識別子（例：com.company.profile）
com.example.profile.contractor

組織
プロファイルの組織名
Example Inc.

説明
プロファイルの内容や目的の概要
Configuration profile for contract employees.

セキュリティ
プロファイルをいつ取り除くかを制御します
常に確認

指定する名前は、プロファイルリストに表示され、プロファイルがインストールされた後のデバイスに表示されます。一意の名前である必要はありませんが、プロファイルを識別できる分かりやすい名前を使用することをお勧めします。

プロファイル識別子は、このプロファイルを一意に識別できるものでなければなりません。また、com.companyname.identifier フォーマットを使用する必要があります。identifier がプロファイルになります。（例：com.mycompany.homeoffice）

識別子は重要です。プロファイルをインストールするときに、値がデバイス上の既存のプロファイルと比較されるためです。識別子が一意の場合は、プロファイル内の情報がデバイスに追加されます。識別子がすでにインストール済みのプロファイルと一致する場合、Exchange 設定の場合を除いて、プロファイル内の情報によってすでにデバイス上にある設定が置き換えられます。Exchange アカウントを変更するには、アカウントに関連するデータを消去できるように、最初にプロファイルを手動で削除する必要があります。

ユーザがデバイスにインストールされているプロファイルを削除できないようにするには、「セキュリティ」ポップアップメニューからオプションを選択します。「認証時」オプションでは、デバイス上のプロファイルの削除を許可するための認証パスワードを指定できます。「なし」オプションを指定した場合、プロファイルを新しいバージョンにアップデートすることはできますが、削除することはできません。

パスコード設定

Exchange パスコードポリシーを使用しない場合は、このペイロードを使用してデバイスポリシーを設定します。デバイスを使用するときにパスコードを要求するかどうかを指定したり、パスコードの特性や変更頻度を指定することもできます。構成プロファイルが読み込まれた直後に、ユーザは設定済みポリシーに準拠したパスコードの入力を求められます。入力しない場合は、プロファイルはインストールされません。

デバイスポリシーと Exchange パスコードポリシーを使用する場合は、2 つのポリシーが結合され、厳しい方の設定が適用されます。対応している Exchange ActiveSync ポリシーについては、8 ページの「Microsoft Exchange ActiveSync」を参照してください。

以下のポリシーを設定できます：

- **デバイスのパスコードが必要：** デバイスを使用する前に、パスコードを入力することをユーザに要求します。入力しない場合は、そのデバイスを手にするすべての人がその機能とデータにアクセスできます。
- **単純値を許可：** パスコードに連続する文字や反復する文字を使用することをユーザに許可します。たとえば、「3333」や「DEFG」のようなパスコードが許可されます。
- **英数字の値が必要：** パスコードに少なくとも 1 つの英字を含める必要があります。
- **最小のパスコード長：** パスコードの最小文字数を指定します。
- **複合文字の最小数：** パスコードに必要な英数字以外の文字（$、&、および !）の数。
- **パスコードの有効期限（日数）：** 指定した間隔でユーザがパスコードを変更することを要求します。

- 自動ロック（分数設定）： デバイスがこの期間使用されない場合は、自動的にロックされます。パスコードを入力すると、ロック解除されます。
- 失敗再試行の最大数： デバイスがワイプされるまでに試行できるパスコード誤入力の回数を決定します。この設定を変更しない場合は、パスコードの入力に 6 回失敗すると、一定の時間が経過するまでパスコードを入力できなくなります。待機時間は、入力に失敗するたびに長くなります。入力に 11 回失敗すると、すべてのデータと設定がデバイスから安全に消去されます。パスコードの入力に 6 回失敗した後は、常に一定の時間が経過するまで入力できない状態になります。つまり、この値を 6 以下に設定した場合は、入力できない時間がなくなり、設定した値を超えるとすぐにデバイスが消去されることになります。
- パスコードの履歴： 新しいパスコードが以前に使用したパスコードと一致した場合、そのパスコードは受け入れられません。以前のパスワードと比較できるよう、記憶する以前のパスコードの数を指定できます。
- デバイスのロックの猶予期間： パスコードの再入力を求めずに、使用後どれくらいでデバイスのロックを解除できるかを指定します。

制限の設定

ユーザが使用できるデバイス機能を指定するには、このペイロードを使用します。

- 露骨な内容を許可： これをオフにすると、iTunes Store から購入した露骨な内容の音楽やビデオが隠されます。露骨な内容は、iTunes Store から販売されるときに、レコード会社などのコンテンツプロバイダによって露骨な内容として指定されています。
- 「Safari」の使用を許可： このオプションをオフにすると、Safari Web ブラウザアプリケーションは無効になり、アイコンがホーム画面から削除されます。ユーザが Web クリップを開くこともできなくなります。
- YouTube の使用を許可： このオプションをオフにすると、YouTube ブラウザアプリケーションは無効になり、アイコンがホーム画面から削除されます。
- iTunes Music Store の使用を許可： このオプションをオフにすると、iTunes Music Store は無効になり、アイコンがホーム画面から削除されます。ユーザはコンテンツをプレビュー、購入、およびダウンロードできません。
- アプリケーションのインストールを許可： このオプションをオフにすると、App Store は無効になり、アイコンがホーム画面から削除されます。ユーザはアプリケーションをインストールまたはアップデートできません。
- カメラの使用を許可： このオプションをオフにすると、カメラは完全に無効になり、アイコンがホーム画面から削除されます。ユーザは写真を撮ることはできません。
- 画面の取り込みを許可：このオプションをオフにすると、ユーザはディスプレイのスクリーンショットを保存できません。

Wi-Fi 設定

デバイスをワイヤレスネットワークに接続する方法を設定するときは、このペイロードを使用します。編集パネルで「追加」（＋）ボタンをクリックすることで、複数のネットワーク構成を追加できます。

ユーザが接続を開始するには、これらの設定が指定されていて、ネットワークの要件を満たしている必要があります。

- サービスセット識別子： 接続先のワイヤレスネットワークの SSID を入力します。
- 非公開ネットワーク： ネットワークからその識別子をブロードキャストするかどうかを指定します。
- セキュリティの種類： ネットワークの認証方法を選択します。以下のオプションは、パーソナルネットワークとエンタープライズネットワークの両方で選択できます。
  - なし： 認証を使用しません。
  - WEP： WEP 認証のみを使用します。
  - WPA/WPA 2： WPA 認証のみを使用します。
  - Any： ネットワークに接続するときに WEP または WPA 認証を使用します。ただし、認証されていないネットワークには接続しません。
- パスワード： ワイヤレスネットワークに接続するためのパスワードを入力します。これを空白のままにしておくと、ユーザにパスワードの入力が求められます。

エンタープライズ設定

このセクションでは、エンタープライズネットワークに接続するための設定を指定します。これらの設定は、「セキュリティの種類」ポップアップメニューで「エンタープライズ設定」を選択したときに表示されます。

「プロトコル」タブでは、「受け入れた EAP の種類」を指定し、EAP-FAST PAC（Protected Access Credential）設定を構成します。

「認証」タブでは、ユーザ名や認証プロトコルなどのサインイン設定を指定します。「資格情報」セクションを使用して固有名をインストールした場合は、「固有名証明書」ポップアップメニューからその固有名証明書を選択できます。

「信頼」タブでは、Wi-Fi 接続用の認証サーバを検証するために、どの証明書を信頼できる証明書として扱うかを指定します。「信頼できる証明書」リストには、「資格情報」タブを使用して追加した証明書が表示され、信頼できる証明書として扱う証明書を選択できます。信頼できる認証サーバの名前を「信頼できるサーバ証明書の名前」リストに追加します。特定のサーバ（server.mycompany.com など）または一部の名前（*.mycompany.com など）を指定できます。

「信頼例外を許可」オプションでは、信頼チェーンを確立できないときでも、ユーザがサーバを信頼するかどうかを決定することを許可できます。このような確認画面が表示されないようにして、信頼できるサービスだけに接続することを許可するときは、このオプションを無効にして、必要な証明書をすべてプロファイルに埋め込んでください。

VPN 設定

ネットワークに接続するための VPN 設定を入力するときは、このペイロードを使用します。「追加」（＋）ボタンをクリックすることで、複数の VPN 接続を追加できます。

対応している VPN プロトコルと認証方法については、10 ページの「VPN」を参照してください。選択できるオプションは、選択したプロトコルと認証方法によって異なります。

VPN オンデマンド

証明書ベースの IPSec 構成では、特定のドメインにアクセスすると VPN 接続が自動的に確立されるように、VPN オンデマンドをオンにすることができます。

VPN オンデマンドのオプションは以下の通りです：

設定	説明
常に確立	指定したドメインに一致するアドレスがある場合は、そのための VPN 接続を開始します。
確立しない	指定したドメインと一致するアドレスがあっても、そのための VPN 接続は開始しません。ただし、VPN がすでにアクティブの場合は、それが使用されることがあります。
必要に応じて確立	DNS ルックアップが失敗した後でのみ、指定したドメインと一致するアドレスで VPN 接続を開始します。

この動作は、一致するすべてのアドレスに適用されます。アドレスの比較には、末尾から先頭方向への単純な文字列一致が使用されます。アドレス「.example.org」は、「support.example.org」や「sales.example.org」と一致しますが、「www.private-example.org」とは一致しません。ただし、一致するドメインを「example.com」と指定した場合は（先頭にピリオドがないことに注目してください）、「www.private-example.com」などとも一致します。

LDAP 接続は VPN 接続を開始しないことに注意してください。VPN が「Safari」などの別のアプリケーションによってすでに確立されてない場合、LDAP ルックアップは失敗します。

VPN プロキシ

iPhone は、手動の VPN プロキシと、PAC または WPAD を使用した自動プロキシ構成に対応しています。VPN プロキシを指定するときは、「プロキシ設定」ポップアップメニューからオプションを選択します。

PAC ベースの自動プロキシ構成の場合、ポップアップメニューから「自動」を選択し、PAC ファイルの URL を入力します。PACS 機能とファイルフォーマットについては、56 ページの「その他の参考資料」を参照してください。

WPAD（Web プロキシ自動検出）構成の場合、ポップアップメニューから「自動」を選択します。「プロキシサーバの URL」フィールドは空のままにします。iPhone で DHCP と DNS を使用して WPAD ファイルが要求されます。WPAD については、56 ページの「その他の参考資料」を参照してください。

メール設定

ユーザの POP または IMAP メールアカウントを構成するときは、このペイロードを使用します。Exchange アカウントを追加する場合は、次の「Exchange 設定」を参照してください。

プロファイルに指定したメール設定の一部（アカウント名、パスワード、および代替SMTP サーバなど）は、ユーザが変更できます。プロファイルにこれらの情報を入力しなかった場合は、ユーザがアカウントにアクセスするときにその情報の入力が求められます。

「追加」（＋）ボタンをクリックすることで、複数のメールアカウントを追加できます。

Exchange 設定

ユーザの Exchange サーバ設定を入力するときは、このペイロードを使用します。ユーザ名、ホスト名、およびメールアドレスを指定することで、そのユーザのプロファイルを作成できます。ホスト名だけを指定した場合は、ユーザがプロファイルをインストールするときにほかの値の入力を求められます。

プロファイルにユーザ名、ホスト名、および SSL 設定を指定した場合は、ユーザはデバイス上でこれらの設定を変更できなくなります。

各デバイスで構成できる Exchange アカウントは 1 つだけです。IMAP を介した Exchange アカウントなどのその他のメールアカウントは、Exchange アカウントを追加しても影響されません。プロファイルを使用して追加された Exchange アカウントは、そのプロファイルを削除したときに削除されます。それ以外の場合は削除できません。

デフォルトでは、Exchange の連絡先、カレンダー、およびメールが同期されます。ユーザはデバイス上でこれらの設定（何日分のデータを同期するかなど）を「設定」＞「メール / 連絡先 / カレンダー」＞「アカウント」と移動して変更できます。

「SSL を使用」オプションを選択する場合は、「資格情報」パネルを使用して、接続を認証するために必要な証明書を必ず追加してください。

ユーザを識別する証明書を Exchange ActiveSync Server に提供するには、「追加」（＋）ボタンをクリックし、Mac OS X のキーチェーンまたは Windows の証明書ストアから固有名証明書を選択します。証明書を追加した後に、認証資格情報名を指定できます（ActiveSync 構成に必要な場合）。構成プロファイルに証明書のパスフレーズに埋め込むこともできます。パスフレーズを埋め込まない場合は、ユーザはプロファイルのインストール時にパスフレーズの入力を求められます。

LDAP 設定
LDAPv3 ディレクトリに接続するための設定を入力するには、このペイロードを使用します。ディレクトリごとに複数の検索ベースを指定できます。また、「追加」（＋）ボタンをクリックすることで、複数のディレクトリ接続を構成できます。

「SSL を使用」オプションを選択する場合は、「資格情報」パネルを使用して、接続を認証するために必要な証明書を必ず追加してください。

CalDAV 設定
CalDAV 準拠のカレンダーサーバに接続するためのアカウント設定を提示するには、このペイロードを使用します。これらのアカウントはデバイスに追加されます。Exchange アカウントと同様に、プロファイルをインストールするときにプロファイルに入力しなかった情報（アカウントパスワードなど）は、ユーザが手動で入力する必要があります。

「SSL を使用」オプションを選択する場合は、「資格情報」パネルを使用して、接続を認証するために必要な証明書を必ず追加してください。

「追加」（＋）ボタンをクリックすることで、複数のメールアカウントを設定できます。

照会するカレンダーの設定
デバイスのカレンダーアプリケーションに読み取り専用の照会カレンダーを追加するには、このペイロードを使用します。「追加」（＋）ボタンをクリックすることで、複数の登録を設定できます。

照会できる公開カレンダーのリストについては、
www.apple.com/downloads/macosx/calendars を参照してください。

「SSL を使用」オプションを選択する場合は、「資格情報」パネルを使用して、接続を認証するために必要な証明書を必ず追加してください。

Web クリップ設定
ユーザのデバイスのホーム画面に Web クリップを追加するには、このペイロードを使用します。Web クリップにより、よく使う Web ページにすばやくアクセスできます。

入力する URL には接頭辞 http:// または https:// を必ず付けてください。これは、Web クリップを正しく機能させるために必要です。たとえば、オンライン版の「iPhone ユーザガイド」をホーム画面に追加するときは、Web クリップの URL：http://help.apple.com/iphone/ を指定します。

独自のアイコンを追加するときは、gif、jpeg、または png フォーマットの、サイズが 59 × 60 ピクセルのグラフィックファイルを選択します。イメージは、自動的にサイズ調整され、必要に応じて png フォーマットに変換されます。

資格情報の設定

デバイスに証明書と固有名を追加するときは、このペイロードを使用します。対応しているフォーマットについては、11 ページの「証明書と固有名」を参照してください。

資格情報をインストールするときに、デバイス上にある信頼された証明書へのチェーンを確立するために必要な中間証明書もインストールしてください。インストール済みのルートのリストについては、アップルのサポート記事（http://support.apple.com/kb/HT2185?viewlocale=ja_JP）を参照してください。

Microsoft Exchange で使用する固有名を追加する場合は、代わりに Exchange ペイロードを使用してください。36 ページの「Exchange 設定」を参照してください。

Mac OS X で資格情報を追加する：

1 「追加」（＋）ボタンをクリックします。

2 表示されるファイルダイアログで、PKCS1 ファイルまたは PKSC12 ファイルを選択し、「開く」をクリックします。

証明書または固有名をキーチェーンにインストールしたい場合は、「キーチェーンアクセス」を使用して .p12 フォーマットで書き出します。「キーチェーンアクセス」は「/ アプリケーション / ユーティリティ」にあります。ヘルプについては、「キーチェーンアクセス」を開いているときに、「ヘルプ」メニューから「キーチェーンアクセスヘルプ」を参照してください。

構成プロファイルに複数の資格情報を追加するには、もう一度を「追加」（＋）ボタンをクリックします。

Windows で資格情報を追加する：

1 「追加」（＋）ボタンをクリックします。

2 Windows 証明書ストアからインストールしたい資格情報を選択します。

個人用証明書ストアにある資格情報は、使用可能でない場合は追加する必要があり、秘密鍵を書き出し可能と指定する必要があります。これは、証明書のインポートウィザードで提示される手順の 1 つです。ルート証明書を追加するにはコンピュータへの管理アクセスが必要であり、証明書を個人用ストアに追加する必要があることに注意してください。

複数の構成プロファイルを使用する場合は、証明書が複製されないようにしてください。同じ証明書の複数のコピーをインストールすることはできません。

構成プロファイルを使って証明書をインストールする代わりに、ユーザが「Safari」を使用して Web ページから証明書をデバイスに直接ダウンロードすることを許可できます。証明書をユーザにメールで送信することもできます。詳しくは、55 ページの「固有名とルート証明書をインストールする」を参照してください。また、SCEP 設定（以下を参照）を使用して、プロファイルをインストールするときに無線で証明書を取得する方法を指定します。

SCEP 設定

SCEP ペイロードでは、デバイスで SCEP（Simple Certificate Enrollment Protocol）を使用して CA から証明書を取得するための設定を指定できます。

設定	説明
URL	これは SCEP サーバのアドレスです。
名前	これは、認証局が解釈する文字列にすることができ、たとえばインスタンス間の区別に使用できます。
サブジェクト	OID および値の配列として表される X.500 名の表現。たとえば、「/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar」です。これは以下のように変換されます： [[["C", "US"]], [["O", "Apple Inc."]], ..., [["1.2.5.3", "bar"]]]
チャレンジ	SCEP サーバが要求またはユーザを識別するために使用できる事前共有シークレット。
鍵のサイズと使用法	鍵のサイズと、このフィールドの下のチェックボックスを使用して鍵の使用条件を選択します。
フィンガープリント	HTTP を使用する認証局の場合は、このフィールドを使って CA の証明書のフィンガープリントを渡します。デバイスは登録処理中にこれを使って CA の応答の真正性を確認します。SHA1 または MD5 フィンガープリントを入力するか、証明書を選択してその署名を読み込むことができます。

iPhone で証明書をワイヤレスで取得する方法については、22 ページの「無線での登録と構成」を参照してください。

詳細設定

詳細ペイロードでは、デバイスの APN（アクセスポイント名）とパケット通信のプロキシ設定を変更できます。これらの設定には、デバイスからキャリアのネットワークに接続する方法を定義します。これらの設定は、キャリアのネットワーク技術者から指示があった場合にのみ変更してください。これらの設定が正しくない場合は、デバイスからパケット通信を使用してデータにアクセスすることはできません。これらの設定が誤って変更された場合に、それらを取り消すときは、デバイスからそのプロファイルを削除してください。APN 設定は、ほかのエンタープライズ設定とは異なる構成プロファイル内に定義することをお勧めします。APN 情報を指定するプロファイルは、携帯電話サービスプロバイダの署名を受ける必要があるためです。

iPhone OS は、最大 20 文字の APN ユーザ名と、最大 32 文字のパスワードに対応しています。

構成プロファイルを編集する

「iPhone 構成ユーティリティ」では、構成プロファイルリストでプロファイルを選択し、ペイロードリストと編集パネルを使って変更を行います。「ファイル」＞「ライブラリに追加」と選択して .mobileconfig ファイルを選択することによって、プロファイルを読み込むこともできます。設定パネルが表示されていない場合は、「表示」＞「詳細情報を表示」と選択します。

デバイスの「一般」ペイロードの「識別子」フィールドは、新しいプロファイルなのか既存のプロファイルへのアップデートなのかを判別するために使用します。ユーザが以前にインストールしたプロファイルをアップデートされたプロファイルで置き換えたい場合は、識別子を変更しないでください。

プロビジョニングプロファイルおよびアプリケーションをインストールする

「iPhone 構成ユーティリティ」では、コンピュータに接続されているデバイス上にアプリケーションと配信プロビジョニングプロファイルをインストールできます。詳しくは、63 ページの第 5 章「アプリケーションを配備する」を参照してください。

構成プロファイルをインストールする

プロファイルを選択したら、デバイスを接続し、「iPhone 構成ユーティリティ」を使用してプロファイルをインストールすることができます。

または、メールでプロファイルをユーザに配信したり、Web ページに投稿することによって配信することもできます。ユーザがデバイスを使ってメールメッセージを開いたとき、または Web からプロファイルをダウンロードしたときに、インストール処理を開始することを求められます。

iPhone 構成ユーティリティを使用して構成プロファイルをインストールする

構成プロファイルは、iPhone OS 3.0 以降にアップデート済みでコンピュータに接続されているデバイス上に、直接インストールできます。「iPhone 構成ユーティリティ」を使用して、以前にインストールしたプロファイルを削除することもできます。

構成プロファイルをインストールするには：

1 USB ケーブルを使って、デバイスをコンピュータに接続します。

しばらくすると、「iPhone 構成ユーティリティ」 のデバイスリストにデバイスが表示されます。

2 デバイスを選択して、「構成プロファイル」タブをクリックします。

3 リストから構成プロファイルを選択して、「インストール」をクリックします。

4 デバイスで「インストール」をタップして、プロファイルをインストールします。

USB を使用してデバイス上に直接インストールすると、構成プロファイルは、デバイスに転送される前に自動的に署名されて暗号化されます。

構成プロファイルをメールで配信する

メールを使って構成プロファイルを配信することができます。ユーザは、デバイスでメッセージを受信し、添付ファイルをタップしてインストールすることによって、プロファイルをインストールします。

構成プロファイルをメール送信するには：

1 「iPhone 構成ユーティリティ」ツールバーの「共有」ボタンをクリックします。

表示されるダイアログで、セキュリティオプションを選択します：

a なし： 標準テキストの .mobileconfig ファイルが作成されます。任意のデバイス上にインストールできます。ファイル内の内容の一部は、ファイルが調べられた場合の情報の漏洩を防ぐために暗号化されます。

b 構成プロファイルに署名： .mobileconfig ファイルは署名されます。変更を加えると、デバイスにはインストールされなくなります。一部のフィールドは、ファイルが調べられた場合の情報の漏洩を防ぐために暗号化されます。インストールされたプロファイルをアップデートできるのは、同じ識別子を持ち、「iPhone 構成ユーティリティ」の同じコピーによって署名されたプロファイルのみになります。

c プロファイルに署名して暗号化： プロファイルに署名して変更できないようにし、内容をすべて暗号化して、プロファイルを調べることができず、特定のデバイスにインストールすることしかできないようにします。プロファイルにパスワードが含まれている場合は、このオプションが推奨されます。デバイスリストから選択するデバイスごとに、別個の .mobileconfig ファイルが作成されます。リストに表示されないデバイスは、暗号化鍵を取得できるように以前にコンピュータに接続されていなかったデバイスか、iPhone OS 3.0 以降にアップグレードされていなかったデバイスです。

2 「共有」をクリックすると、「Mail」（Mac OS X）または「Outlook」（Windows）の新しいメッセージが開きます。追加したプロファイルは圧縮されていない添付ファイルとして表示されます。プロファイルを認識してインストールするには、このファイルをデバイス用に圧縮解除する必要があります。

構成プロファイルを Web 上に配信する

Web サイトを使って構成プロファイルを配信することができます。ユーザは、デバイス上の「Safari」を使用してダウンロードすることによって、構成プロファイルをインストールします。ユーザに URL を簡単に配信するには、SMS 経由で送信します。

構成プロファイルを書き出すには：

1 「iPhone 構成ユーティリティ」ツールバーの「書き出す」ボタンをクリックします。

表示されるダイアログで、セキュリティオプションを選択します：

a なし： 標準テキストの .mobileconfig ファイルが作成されます。任意のデバイス上にインストールできます。ファイル内の内容の一部は、ファイルが調べられた場合の情報の漏洩を防ぐために暗号化されます。ただし、ファイルを Web サイト上に置くときは、必ず認証されたユーザしかアクセスできないようにしてください。

b 構成プロファイルに署名： .mobileconfig ファイルは署名されます。変更を加えると、デバイスにはインストールされなくなります。インストールされたプロファイルをアップデートできるのは、同じ識別子を持ち、「iPhone 構成ユーティリティ」の同じコピーによって署名されたプロファイルのみになります。ファイル内の情報の一部は、ファイルが調べられた場合の情報の漏洩を防ぐために暗号化されます。ただし、ファイルを Web サイト上に置くときは、必ず認証されたユーザしかアクセスできないようにしてください。

c プロファイルに署名して暗号化： プロファイルに署名して変更できないようにし、内容をすべて暗号化して、プロファイルを調べることができず、特定のデバイスにインストールすることしかできないようにします。デバイスリストから選択するデバイスごとに、別個の .mobileconfig ファイルが作成されます。

2 「書き出す」をクリックして、.mobileconfig ファイルを保存する場所を選択します。

ファイルは Web サイト上に投稿できる状態になります。.mobileconfig ファイルは圧縮したり拡張子を変更したりしないでください。デバイスでプロファイルが認識またはインストールされなくなります。

ダウンロードした構成ファイルのユーザによるインストール

ユーザがデバイス上にプロファイルをダウンロードするための URL をユーザに知らせるか、またはユーザがデバイスを使ってアクセスできるメールアカウントにプロファイルを送信したら、エンタープライズ固有の情報を設定できる状態になります。

ユーザがプロファイルを Web からダウンロードしたり、「メール」を使用して添付ファイルを開いたりすると、拡張子 .mobileconfig がデバイスによりプロファイルとして認識され、ユーザが「インストール」をタップするとインストールが始まります。

インストール中に、ユーザは必要な情報の入力を求められます（プロファイルに指定されていないパスワードなど、管理者が指定した設定に必要なその他の情報）。

デバイスには、サーバから Exchange ActiveSync ポリシーが取り込まれます。ポリシーが変更されている場合は、接続のたびに更新されます。デバイスまたは Exchange ActiveSync ポリシーによってパスコード設定が適用される場合は、ユーザはポリシーに準拠するパスコードを入力しないとインストールを完了できません。

さらに、ユーザはプロファイルに含まれている証明書を使用するために必要なパスワードを入力することを求められます。

インストールが正常に完了しない場合は、Exchange サーバに接続できなかったか、またはユーザが処理をキャンセルした可能性があります。そのような場合、ユーザが入力した情報は保持されません。

ユーザは、何日分のメッセージをデバイスに同期するか、または受信ボックス以外にどのメールフォルダを同期するかを変更することができます。デフォルトは 3 日分とすべてのフォルダです。ユーザは「設定」＞「メール / 連絡先 / カレンダー」＞「Exchange アカウント名」と選択することで、これらを変更できます。

構成プロファイルを取り除く／アップデートする

構成プロファイルのアップデートはユーザにプッシュされません。アップデートしたプロファイルをインストールするには、そのユーザに配信します。プロファイル識別子が一致している場合、さらに署名済みの場合は「iPhone 構成ユーティリティ」の同じコピーによって署名されている場合、新しいプロファイルによってデバイス上のプロファイルが置き換えられます。

構成ファイルによって適用される設定は、デバイス上で変更できません。設定を変更するには、アップデートされたプロファイルをインストールする必要があります。プロファイルが署名された場合、それを置き換えることができるのは「iPhone 構成ユーティリティ」の同じコピーによって署名されたプロファイルのみになります。アップデートしたプロファイルが置き換えとして認識されるようにするためには、両方のプロファイル内の識別子が一致する必要があります。識別子については、31 ページの「一般設定」を参照してください。

重要：構成プロファイルを取り除くと、ポリシー、デバイス上に保存されているExchange アカウントのすべてのデータ、およびプロファイルに関連付けられている VPN 設定、証明書、メールメッセージなどのその他の情報が取り除かれます。

プロファイルの一般設定ペイロードで、ユーザによる削除ができないと指定した場合、「削除」ボタンは表示されなくなります。設定が認証パスワードを使用した削除を許可する場合、ユーザは「削除」をタップした後にパスワードの入力を求められます。プロファイルのセキュリティ設定については、31 ページの「一般設定」を参照してください。

デバイスを手動で構成する 3

この章では、iPhone、iPod touch、および iPad を手動で構成する方法について説明します。

自動構成プロファイルをユーザに提供しない場合は、ユーザはデバイスを手動で構成することになります。パスコードポリシーなどの一部の設定は、構成プロファイルを使用しないと設定できません。

VPN 設定

VPN 設定を変更するときは、「設定」＞「一般」＞「ネットワーク」＞「VPN」と移動します。

VPN 設定を構成するときは、VPN サーバから返された情報を基にしてデバイスに設定を入力することを求められます。たとえば、サーバが RSA SecurID トークンを必要とする場合は、RSA SecurID トークンを入力する必要があります。

証明書ベースの VPN 接続を構成するときは、対応する証明書がデバイスにインストールされている必要があります。詳しくは、55 ページの「固有名とルート証明書をインストールする」を参照してください。

VPN オンデマンドはデバイス上では構成できず、構成プロファイルを使用して設定する必要があります。35 ページの「VPN オンデマンド」を参照してください。

VPN プロキシ設定

すべての構成用に 1 つの VPN プロキシを指定することもできます。すべての接続に 1 つのプロキシを構成するには、「手動」をタップし、必要に応じてアドレス、ポート、および認証を指定します。デバイスに自動プロキシ構成ファイルを提供するには、「自動」をタップして PACS ファイルの URL を指定します。WPAD を使用して自動プロキシ構成を指定するには、「自動」をタップします。デバイスが WPAD 設定用の DHCP と DNS を照会します。PACS ファイルのサンプルと参考資料については、この章の最後にある「その他の参考資料」を参照してください。

Cisco IPSec 設定

Cisco IPSec VPN をデバイスに手動で構成するときは、次のような画面が表示されます：

次の表を使って、入力する設定と情報を確認してください：

フィールド	説明
説明	これらの設定を説明するタイトル。
サーバ	接続する VPN サーバの DNS 名または IP アドレス。
アカウント	ユーザの VPN ログインアカウントのユーザ名。グループ名をこのフィールドに入力しないでください。
パスワード	ユーザの VPN ログインアカウントのパスフレーズ。RSA SecurID および CryptoCard 認証の場合、またはユーザが接続しようとするたびにパスワードを手動で入力することを求める場合は、空白のままにします。
証明書を使用	リモートアクセスのためにプロビジョニングされた証明書とその証明書の秘密鍵が含まれた .p12 または .pfx 固有名をインストールした場合にだけ構成できます。「証明書を使用」がオンのときは、「グループ名」および「共有シークレット」フィールドは「固有名」フィールドになり、インストール済みの VPN 互換の固有名のリストから選択します。
グループ名	ユーザが割り当てられているグループの名前。VPN サーバに定義されています。
シークレット	グループの共有シークレット。ユーザが割り当てられているグループのすべてのメンバーに共通です。これはユーザのパスワードではありません。接続を開始するときに指定する必要があります。

PPTP 設定

PPTP VPN をデバイスに手動で構成するときは、次のような画面が表示されます：

次の表を使って、入力する設定と情報を確認してください：

フィールド	説明
説明	これらの設定を説明するタイトル。
サーバ	接続する VPN サーバの DNS 名または IP アドレス。
アカウント	ユーザの VPN ログインアカウントのユーザ名。
RSA SecurID	RSA SecurID トークンを使用する場合は、このオプションをオンにします。すると「パスワード」フィールドが隠されます。
パスワード	ユーザの VPN ログインアカウントのパスフレーズ。
暗号化レベル	デフォルトは「自動」です。その場合、利用できる暗号化レベルのうち、最も高いレベルが選択されます（128 ビット、40 ビット、または「なし」）。「最大」は 128 ビットだけです。「なし」は、暗号化が無効になります。
すべての信号を送信	デフォルトは「オン」です。すべてのネットワークトラフィックを VPN リンク経由で送信します。無効にすると、スプリット・トンネリングが有効になり、VPN 内のサーバに送信されたトラフィックだけがサーバ経由で送信されます。その他のトラフィックは直接インターネットに送信されます。

L2TP 設定

L2TP VPN をデバイスに手動で構成するときは、次のような画面が表示されます：

次の表を使って、入力する設定と情報を確認してください：

フィールド	説明
説明	これらの設定を説明するタイトル。
サーバ	接続する VPN サーバの DNS 名または IP アドレス。
アカウント	ユーザの VPN ログインアカウントのユーザ名。
パスワード	ユーザの VPN ログインアカウントのパスワード。
シークレット	L2TP アカウントの共有シークレット（事前共有キー）。すべての LT2P ユーザに共通です。
すべての信号を送信	デフォルトは「オン」です。すべてのネットワークトラフィックを VPN リンク経由で送信します。無効にすると、スプリット・トンネリングが有効になり、VPN 内のサーバに送信されたトラフィックだけがサーバ経由で送信されます。その他のトラフィックは直接インターネットに送信されます。

Wi-Fi 設定

Wi-Fi 設定を変更するときは、「設定」＞「一般」＞「ネットワーク」＞「Wi-Fi」と移動します。追加するネットワークが通信圏内にある場合は、利用できるネットワークのリストから選択します。それ以外の場合は、「その他」をタップします。

ネットワーク環境で使用されている認証と暗号化に iPhone と iPod touch が対応していることを確認してください。仕様については、11 ページの「ネットワークセキュリティ」を参照してください。認証に必要な証明書のインストールについては、55 ページの「固有名とルート証明書をインストールする」を参照してください。

Exchange 設定

各デバイスで構成できる Exchange アカウントは 1 つだけです。Exchange アカウントを追加するときは、「設定」>「メール / 連絡先 / カレンダー」と移動してから、「アカウントを追加」をタップします。「アカウントを追加」画面で、「Microsoft Exchange」をタップします。

デバイスに Exchange を手動で構成するときは、入力する設定と情報を次の表を使って確認してください：

フィールド	説明
メール	ユーザの完全なメールアドレス。
ドメイン	ユーザの Exchange アカウントのドメイン。
ユーザ名	ユーザの Exchange アカウントのユーザ名。
パスワード	ユーザの Exchange アカウントのパスワード。
説明	このアカウントを説明するタイトル。

iPhone、iPod touch、および iPad は Microsoft 社の自動検出サービスに対応しているので、フロントエンド Exchange サーバのアドレスはユーザ名とパスワードによって判別されます。サーバのアドレスを判別できない場合は、アドレスの入力を求められます。

Exchange サーバが 443 以外のポートで接続を待機している場合は、exchange.example.com:ポート番号のフォーマットで「サーバ」フィールドにポート番号を指定します。

Exchange アカウントが正常に構成されると、サーバのパスコードポリシーが適用されます。ユーザの現在のパスコードが Exchange ActiveSync ポリシーに準拠していない場合は、パスコードの変更または設定を求められます。準拠するパスコードを設定するまでは、デバイスは Exchange サーバと通信できません。

次に、Exchange サーバとすぐに同期するかどうかを確認する画面が表示されます。ここで同期しないことを選択した場合でも、後で「設定」＞「メール/ 連絡先 / カレンダー」と選択すれば、カレンダーと連絡先の同期を有効にできます。デフォルトでは、新しいデータがサーバに送信すると、Exchange ActiveSync によってデバイスにプッシュされます。スケジュールに基づいて新しいデータをフェッチしたい場合、または新しいデータの取得を手動だけで行いたい場合は、「設定」＞「メール / 連絡先 / カレンダー」を使って設定を変更します。

何日分のメールメッセージをデバイスに同期するかを変更するときは、「設定」＞「メール / 連絡先 / カレンダー」と移動します。受信ボックス以外に、プッシュメール配信にどのフォルダを含めるかを選択することもできます。

カレンダーデータの設定を変更するには、「設定」＞「メール / 連絡先 / カレンダー」＞「同期」と移動します。

LDAP 設定

iPhone、iPod touch、および iPad では、LDAP ディレクトリサーバ上の連絡先情報を調べることができます。LDAP サーバを追加するときは、「設定」>「メール / 連絡先 / カレンダー」>「アカウントを追加」>「その他」と移動します。その後、「LDAP アカウントを追加」をタップします。

LDAP サーバのアドレスを入力し、必要に応じてユーザ名とパスワードを入力してから、「次へ」をタップします。サーバに接続可能であり、デフォルトの検索設定がデバイスに提供される場合、それらの設定が使用されます。

対応している検索範囲設定は以下の通りです：

検索範囲設定	説明
ベース	ベースオブジェクトのみを検索します。
1 レベル	ベースオブジェクトの 1 レベル下のオブジェクトを検索しますが、ベースオブジェクトそのものは検索しません。
サブツリー	ベースオブジェクトとその下のすべてのオブジェクトのツリー全体を検索します。

サーバごとに複数の検索設定のセットを定義できます。

CalDAV 設定

iPhone、iPod touch、および iPad では、グループのカレンダーやスケジュールを提供する CalDAV カレンダーサーバを利用します。CalDAV サーバを追加するには、「設定」>「メール / 連絡先 / カレンダー」>「アカウントを追加」>「その他」と移動します。その後、「CalDAV アカウントを追加」をタップします。

CalDAV サーバのアドレスを入力し、必要に応じてユーザ名とパスワードを入力してから、「次へ」をタップします。サーバに接続すると、さらにオプションを設定するためのその他のフィールドが表示されます。

カレンダーの照会の設定

プロジェクトスケジュールや休日など、読み取り専用のカレンダーを追加できます。カレンダーを追加するには、「設定」>「メール / 連絡先 / カレンダー」>「アカウントを追加」>「その他」と移動し、「照会するカレンダーを追加」をタップします。

iCalendar（.ics）ファイルの URL と、必要に応じてユーザ名とパスワードを入力してから、「保存」をタップします。カレンダーをデバイスに追加したときに、カレンダー設定されているアラームを削除するかどうかも指定できます。

照会カレンダーを手動で追加するほか、ユーザに webcal:// URL（または .ics ファイルへの http:// リンク）を送信することができます。ユーザがリンクをタップすると、それを照会するカレンダーとして追加するかどうかを確認する画面が表示されます。

固有名とルート証明書をインストールする

プロファイルを使って証明書を配信しない場合は、デバイスを使って Web サイトからダウンロードするか、またはメールメッセージの添付ファイルを開くことによって、ユーザが手動でインストールすることができます。デバイスでは、以下の MIME タイプとファイル拡張子によって証明書が認識されます：

- application/x-pkcs12、.p12、.pfx
- application/x-x509-ca-cert、.cer、.crt、.der

対応しているフォーマットやその他の要件については、11 ページの「証明書と固有名」を参照してください。

証明書または固有名がデバイスにダウンロードされると、「プロファイルをインストール」画面が表示されます。説明にはその種類（固有名または認証局）が表示されます。証明書をインストールするには、「インストール」をタップします。固有名証明書の場合は、証明書のパスワードを入力するよう求められます。

インストールされている証明書を表示または取り除くときは、「設定」＞「一般」＞「プロファイル」と移動します。アカウントまたはネットワークにアクセスするために必要な証明書を取り除いた場合は、デバイスからそれらのサービスに接続することはできません。

メールアカウントを追加する

構成できる Exchange アカウントは 1 つだけですが、 複数の POP および IMAP アカウントを追加することができます。これらは、たとえば、Lotus Notes または Novell Groupwise メールサーバ上のメールにアクセスするために使用できます。「設定」 > 「アカウント」 > 「メール / 連絡先 / カレンダー」 > 「アカウントを追加」 > 「その他」と移動します。IMAP アカウントの追加について詳しくは、「iPhone ユーザガイド」、「iPod touch ユーザガイド」、または「iPad ユーザガイド」を参照してください。

プロファイルをアップデートする／取り除く

構成プロファイルのアップデートまたは削除の方法については、43 ページの「構成プロファイルを取り除く／アップデートする」を参照してください。

配信プロビジョニングプロファイルのインストールについては、63 ページの「アプリケーションを配備する」を参照してください。

その他の参考資料

VPN プロキシ設定で使用する自動プロキシ構成ファイルのフォーマットと関数については、以下の Web サイトを参照してください：

- PAC（プロキシ自動構成）（http://en.wikipedia.org/wiki/Proxy_auto-config）
- Web プロキシ自動検出プロトコル（http://en.wikipedia.org/wiki/Wpad）
- Microsoft TechNet の「Using Automatic Configuration, Automatic Proxy, and Automatic Detection」（http://technet.microsoft.com/en-us/library/dd361918.aspx）

アップルでは、標準的な Web ブラウザで見ることができるビデオチュートリアルをいくつか用意しています。iPhone、iPod touch、および iPad の機能を設定して使用する方法が紹介されています：

- iPhone のビデオガイド（www.apple.com/jp/iphone/guidedtour/）
- iPod touch のビデオガイド（www.apple.com/jp/ipodtouch/guidedtour/）
- iPad のビデオガイド（www.apple.com/ipad/guided-tours/）
- iPhone のサポート Web ページ（www.apple.com/jp/support/iphone/）
- iPod touch のサポート Web ページ（www.apple.com/jp/support/ipodtouch/）
- iPad のサポート Web ページ（www.apple.com/jp/support/ipad/）

また、デバイスごとにユーザガイド（PDF 形式）が用意されており、追加のヒントや使いかたの詳細が記載されています：

- 「iPhoneユーザガイド」：http://manuals.info.apple.com/ja_JP/iPhone_User_Guide_JP.pdf
- 「iPod touch ユーザガイド」：http://manuals.info.apple.com/ja_JP/iPod_touch_2.0_User_Guide_J.pdf
- 「iPad ユーザガイド」：http://manuals.info.apple.com/ja_JP/iPad_User_Guide_JP.pdf

iTunes を配備する

4

「iTunes」を使用して、音楽やビデオを同期したり、アプリケーションをインストールしたりします。

この章では、「iTunes」とエンタープライズアプリケーションを配備する方法について説明し、指定できる設定と制限について明記します。

iPhone、iPod touch、および iPad では、各タイプのデータ（音楽やメディアなど）を一度に 1 台のコンピュータのみに同期できます。たとえば、両方のコンピュータで「iTunes」の同期オプションを適切に設定することで、音楽をデスクトップコンピュータと同期したり、ブックマークをポータブルコンピュータと同期することができます。同期オプションについては、「iTunes」が開いているときに「ヘルプ」メニューから「iTunes ヘルプ」を参照してください。

iTunes をインストールする

「iTunes」では、Macintosh および Windows の標準インストーラが使用されます。最新バージョンとシステム要件のリストは、www.apple.com/jp/itunes からダウンロードできます。

「iTunes」の配信のライセンス要件については、次の Web サイトを参照してください：
http://developer.apple.com/jp/softwarelicensing/agreements/itunes.html

iTunes を Windows コンピュータにインストールする

「iTunes」を Windows コンピュータにインストールすると、デフォルトで最新版の QuickTime、Bonjour、およびアップル・ソフトウェア・アップデートもインストールされます。パラメータを iTunes インストーラに渡すか、またはユーザのコンピュータにインストールしたいコンポーネントだけをプッシュすることで、これらのコンポーネントのインストールを回避できます。

iTunesSetup.exe を使用して Windows にインストールする

「iTunes」の通常のインストール処理を使用するけれども、一部のコンポーネントをインストールしない場合は、コマンドラインを使って iTunesSetup.exe にプロパティを渡すことができます。

プロパティ	説明
NO_AMDS=1	Apple Mobile Device Services をインストールしません。「iTunes」がモバイルデバイスを同期および管理するときに必要です。
NO_ASUW=1	Apple Software Update for Windows をインストールしません。アップルの新しいバージョンのソフトウェアをユーザに通知します。
NO_BONJOUR=1	Bonjour をインストールしません。ネットワーク上のプリンタ、共有 iTunes ライブラリ、およびその他のサービスをゼロ構成で検出します。
NO_QUICKTIME=1	QuickTime をインストールしません。「iTunes」を使用するときに必要です。クライアントコンピュータにすでに最新版がインストールされているかどうか分からない場合は、QuickTime のインストールを回避しないでください。

Windows にサイレントインストールする

「iTunes」をサイレントインストールするには、iTunesSetup.exe から個々の .msi ファイルを抽出してから、ファイルをクライアントコンピュータにプッシュします。

iTunesSetup.exe から .msi ファイルを抽出するには：

1 iTunesSetup.exe を実行します。

2 「%temp%」を開いて「IXPnnn.TMP」という名前のフォルダを見つけます。「%temp%」は一時ディレクトリ、nnn は 3 桁の任意の数字です。Windows XP の場合、一時ディレクトリは通常、「起動ドライブ :\Documents and Settings\ ユーザ \Local Settings\temp\」です。Windows Vista の場合、一時ディレクトリは通常は「\Users\ユーザ \AppData\Local\Temp\」です。

3 このフォルダの .msi ファイルを別の場所にコピーします。

4 iTunesSetup.exe で開いたインストーラを終了します。

それから、Microsoft 管理コンソールの「グループ・ポリシー・オブジェクト・エディタ」を使って、.msi ファイルを「コンピュータの構成」ポリシーに追加します。「ユーザの構成」ポリシーではなく、必ず「コンピュータの構成」ポリシーに追加してください。

重要：「iTunes」には QuickTime と Apple Application Support が必要です。Apple Application Support をインストールしてから「iTunes」をインストールする必要があります。「iTunes」で iPhone、iPad、または iPod touch を使用するには、AMDS（Apple Mobile Device Services）が必要です。

.msi ファイルをプッシュする前に、インストールしたいローカライズ済みの「iTunes」のバージョンを選択する必要があります。これを行うには、bin\ にある ORCA ツール（Windows SDK によって Orca.msi としてインストールされます）で .msi を開きます。次に、概要情報のストリームを編集し、インストールしない言語を削除します。（ロケール ID1033 は英語です。）または、「グループ・ポリシー・オブジェクト・エディタ」を使って、.msi ファイルの配備プロパティを「言語を無視する」に変更します。

iTunes を Macintosh コンピュータにインストールする

Mac コンピュータには「iTunes」がインストールされています。最新バージョンの「iTunes」は www.apple.com/jp/itunes から入手できます。「iTunes」を Mac クライアントにプッシュするには、Mac OS X Server に付属の「ワークグループマネージャ」という管理ツールを使用できます。

iTunes を使ってデバイスをすばやくアクティベーションする

新しい iPhone、iPod touch、または iPad を使用する前に、「iTunes」を実行しているコンピュータに接続してアクティベーションする必要があります。通常は、デバイスをアクティベーションした後に、「iTunes」によってコンピュータに自動的に同期されます。ほかの人のデバイスを設定するときにこの動作を回避するには、アクティベーション専用モードを有効にします。これにより、デバイスがアクティベーションされた後にデバイスが自動的に取り出されます。デバイスは構成できる状態ですが、メディアやデータは入っていません。

Mac OS X でアクティベーション専用モードを有効にするには：

1 「iTunes」が実行中でないことを確認してから、「ターミナル」を開きます。

2 「ターミナル」で、コマンドを入力します：

- アクティベーション専用モードを有効にするには：

```
defaults write com.apple.iTunes StoreActivationMode -integer 1
```

- アクティベーション専用モードを無効にするには：

```
defaults delete com.apple.iTunes StoreActivationMode
```

デバイスをアクティベーションする方法については、後述の「アクティベーション専用モードを使用する」を参照してください。

Windows でアクティベーション専用モードを有効にするには：

1 「iTunes」が実行中でないことを確認してから、コマンドプロンプトウインドウを開きます。

2 コマンドを入力します：

- アクティベーション専用モードを有効にするには：

```
"C:\Program Files\iTunes\iTunes.exe" /setPrefInt StoreActivationMode 1
```

- アクティベーション専用モードを無効にするには：

```
"C:\Program Files\iTunes\iTunes.exe" /setPrefInt StoreActivationMode 0
```

ショートカットを作成するか「iTunes」の既存のショートカットを編集してこれらのコマンドを取り込むことで、アクティベーション専用モードの有効／無効をすばやく切り替えることもできます。

「iTunes」がアクティベーション専用モードであることを確認するには、「iTunes」＞「バージョン情報」と選択し、「iTunes」のバージョンとビルド ID の下に「アクティベーション専用モード」というテキストがあるか確認します。

アクティベーション専用モードを使用する

すでに説明した方法でアクティベーション専用モードを有効にしていることを確認してから、次の手順を実行します。

1 iPhone をアクティベーションする場合は、有効な SIM カードを挿入します。SIM 取り出しツールまたはまっすぐに伸ばしたクリップを使って、SIM トレイを取り出します。詳しくは、「iPhone ユーザガイド」を参照してください。

2 iPhone、iPod touch、または iPad をコンピュータに接続します。デバイスをアクティベーションするには、コンピュータがインターネットに接続されている必要があります。

   必要に応じて「iTunes」が開き、デバイスがアクティベーションされます。デバイスのアクティベーションが成功すると、メッセージが表示されます。

3 デバイスの接続を解除します。

   すぐに別のデバイスを接続してアクティベーションできます。アクティベーション専用モードが有効なデバイスは自動的に同期されません。「iTunes」を使用してデバイスを同期する場合には、アクティベーション専用モードを無効にするのを忘れないでください。

iTunes の制限を設定する

ユーザが「iTunes」の特定の機能を使用することを制限できます。これはペアレンタルコントロールと呼ばれることもあります。以下の機能を制限できます：

- 新しいバージョンの「iTunes」およびデバイスのソフトウェア・アップデートを自動的に確認したりユーザが手動で確認すること
- メディアをブラウズまたは再生しているときに Genius の候補を表示すること
- デバイスを接続しているときに自動的に同期すること
- アルバムアートワークをダウンロードすること
- ビジュアライザプラグインを使用すること
- ストリーミングメディアの URL を入力すること
- Apple TV システムを自動的に検出すること
- 新しいデバイスをアップルに登録すること
- Podcast を登録すること
- インターネットラジオを再生すること
- iTunes Store にアクセスすること
- 「iTunes」も実行しているローカル・ネットワーク・コンピュータとライブラリを共有すること
- 露骨な内容と指定されている iTunes メディアコンテンツを再生すること
- ムービーを再生すること
- テレビ番組を再生すること

Mac OS X のために iTunes 制限を設定する

Mac OS X では、plist ファイルのキーを使ってアクセスを制御します。Mac OS X では、上に記載されているキーの値は、Mac OS X Server に付属の「ワークグループマネージャ」管理ツールを使って「~/Library/Preferences/com.apple.iTunes.plist」を編集することによって、ユーザごとに指定できます。

手順については、アップルのサポート記事（http://docs.info.apple.com/article.html?artnum=303099-ja）を参照してください。

Windows のために iTunes 制限を設定する

Windows では、以下のいずれかのレジストリキー内のレジストリ値を設定することによって、アクセスを制御します：

Windows XP および 32 ビット Windows Vista の場合：

- HKEY_LOCAL_MACHINE\Software\Apple Computer, Inc.\iTunes\[SID]\Parental Controls\
- HKEY_CURRENT_USER\Software\Apple Computer, Inc.\iTunes\Parental Controls

64 ビット Windows Vista の場合：

- HKEY_LOCAL_MACHINE\Software\Wow6432Node\Apple Computer, Inc.\iTunes\[SID]\Parental Controls\
- HKEY_CURRENT_USER\Software\Wow6432Node\Apple Computer, Inc.\iTunes\Parental Controls

「iTunes」のレジストリ値については、アップルのサポート記事（http://support.apple.com/kb/HT2102?viewlocale=ja_JP）を参照してください。

Windows レジストリの編集についての一般的な情報については、Microsoft 社のヘルプおよびサポート記事（http://support.microsoft.com/kb/136393）を参照してください。

iTunes および iPhone OS を手動でアップデートする

「iTunes」でソフトウェア・アップデートを自動的に確認する機能とユーザが手動で確認する機能を無効にした場合は、手動インストール用のソフトウェア・アップデートをユーザに配信する必要があります。

「iTunes」をアップデートするときは、このガイドですでに説明したインストールと配備の手順を参照してください。「iTunes」をユーザに配信する処理と同じ手順です。

iPhone OS をアップデートするときは、以下の手順に従ってください：

1 「iTunes」のソフトウェア・アップデートが無効になっていないコンピュータで、「iTunes」を使ってソフトウェア・アップデートをダウンロードします。これを行うには、「iTunes」に接続されているデバイスを選択し、「概要」タブをクリックしてから、「アップデートを確認」（Mac）または「更新ファイルを確認」（Windows）ボタンをクリックします。

2 ダウンロード後に、以下の場所にあるアップデータファイル（.ipsw）をコピーします：

- Mac OS X の場合： ~/ ライブラリ /iTunes/iPhone Software Updates/
- Windows XP の場合： 起動ドライブ :\Documents and Settings\ <ユーザ> \Application Data\Apple Computer\iTunes\iPhone Software Updates\

3 .ipsw ファイルをユーザに配信するか、ユーザがアクセスできるネットワーク上に置きます。

4 アップデートを適用する前に「iTunes」を使ってデバイスのバックアップを作成するように、ユーザに伝えてください。手動でアップデートするときは、インストールする前にデバイスのバックアップは自動的に作成されません。新しいバックアップを作成するには、「iTunes」のサイドバーでデバイスを右クリックするか（Windows）、Control キーを押したままクリックします（Mac）。次に、表示されるコンテキストメニューから「バックアップ」を選択します。

5 ユーザが、デバイスを「iTunes」に接続してデバイスの「概要」タブを選択することによって、アップデートをインストールします。次にユーザは、Option キー（Mac）または Shift キー（Windows）を押したまま「アップデートを確認」（Mac）または「更新ファイルを確認」（Windows）ボタンをクリックします。

6 ファイルを選択するダイアログが表示されます。ユーザが .ipsw ファイルを選択して「開く」をクリックすると、アップデート処理が開始されるはずです。

iTunes を使ってデバイスのバックアップを作成する

iPhone、iPod touch、または iPad を「iTunes」と同期すると、デバイス設定のバックアップがコンピュータに自動的に作成されます。App Store から購入したアプリケーションは iTunes ライブラリにコピーされます。

独自に開発したアプリケーションを作成し、エンタープライズ配布プロファイルを使ってユーザに配布しても、それらのバックアップが作成されてユーザのコンピュータに転送されることはありません。ただし、そのアプリケーションで作成されるデータファイルはデバイスのバックアップに取り込まれます。

デバイスのバックアップは、「iTunes」の概要パネルでデバイスの「バックアップを暗号化」オプションを選択することで、暗号化されたフォーマットで保存できます。ファイルは AES256 を使って暗号化されます。鍵はセキュリティ保護された状態で iPhone OS のキーチェーンに保存されます。

重要：バックアップするデバイスに暗号化プロファイルがインストールされている場合、「iTunes」ではユーザがバックアップの暗号化を有効にする必要があります。

アプリケーションを配備する

5

iPhone、iPod touch、および iPad のアプリケーションをユーザに配信できます。

開発した iPhone の OS アプリケーションをインストールしたい場合は、アプリケーションをユーザに配信すると、そのユーザが「iTunes」を使ってそのアプリケーションをインストールします。

オンラインの App Store で公開されているアプリケーションは、追加の手順を実行しなくても iPhone、iPod touch、および iPad で使用できます。配信したいアプリケーションを自分で開発する場合は、アップルが発行する証明書を使ってデジタル署名する必要があります。また、配信プロビジョニングプロファイル（ユーザがデバイスでそのアプリケーションを使用することが許可されます）をユーザに提供する必要があります。

独自のアプリケーションを配備する処理は次の手順で構成されます：

- エンタープライズ開発をアップルに登録します。
- 証明書を使ってアプリケーションに署名します。
- 署名したアプリケーションをデバイスで使用することを承認するために、エンタープライズ配信プロビジョニングプロファイルを作成します。
- アプリケーションとエンタープライズ配信プロビジョニングプロファイルをユーザのコンピュータに配備します。
- 「iTunes」を使ってアプリケーションとプロファイルをインストールするようにユーザに指示します。

これらの手順の詳細についてこれから説明します。

アプリケーション開発を登録する

iPhone OS 向けのカスタムアプリケーションを開発および配信するには、まず http://developer.apple.com/jp で「iPhone Enterprise Developer Program」に登録します。

登録処理が完了すると、アプリケーションをデバイスで使用することを許可する指示が届きます。

アプリケーションに署名する

ユーザに配信するアプリケーションには、配信証明書を使って署名する必要があります。証明書を取得して使用する方法については、http://developer.apple.com/jp/iphone/program の「iPhone Dev Center」を参照してください。

配信プロビジョニングプロファイルを作成する

配信プロビジョニングプロファイルがあれば、ユーザがデバイスで使用できるアプリケーションを作成できます。特定のアプリケーションまたは複数のアプリケーションのエンタープライズ配信プロビジョニングプロファイルを作成するときは、プロファイルによって承認される AppID を指定してください。ユーザがアプリケーションを持っていても、それを使用することを承認するプロファイルがない場合、ユーザはそのアプリケーションを使用できません。

エンタープライズ向けのチームエージェントが、「Enterprise Program Portal」（http://developer.apple.com/jp/iphone/program）で配信プロビジョニングプロファイルを作成できます。詳しくは、Web サイトを参照してください。

エンタープライズ配信プロビジョニングプロファイルを作成したら、.mobileprovision ファイルをダウンロードしてから、アプリケーションと一緒にセキュリティ保護された方法で配信します。

iTunes を使用してプロビジョニングプロファイルをインストールする

ユーザの環境に「iTunes」がインストールされていれば、このセクションで定義する以下のフォルダにあるプロビジョニングプロファイルが自動的にインストールされます。フォルダが存在しない場合は、以下に示す名前を使ってフォルダを作成してください。

Mac OS X

- ~/ ライブラリ /MobileDevice/Provisioning Profiles/
- / ライブラリ /MobileDevice/Provisioning Profiles/
- 「~/ ライブラリ /Preferences/com.apple.itunes」内の ProvisioningProfilesPath キーに指定されているパス

Windows XP

- 起動ドライブ :\Documents and Settings\ <ユーザ名> \Application Data\Apple Computer\MobileDevice\Provisioning Profiles
- 起動ドライブ :\Documents and Settings\All Users\Application Data\Apple Computer\MobileDevice\Provisioning Profiles
- 「SOFTWARE\Apple Computer, Inc\iTunes」内の ProvisioningProfilesPath レジストリキーの HKCU または HKLM に指定されているパス

Windows Vista

- 起動ドライブ :\Users\ <ユーザ名> \AppData\Roaming\Apple Computer\MobileDevice\Provisioning Profiles
- 起動ドライブ :\ProgramData\Apple Computer\MobileDevice\Provisioning Profiles
- 「SOFTWARE\Apple Computer, Inc\iTunes」内の ProvisioningProfilesPath レジストリキーの HKCU または HKLM に指定されているパス

上記の場所にあるプロビジョニングプロファイルは、「iTunes」によって同期されるデバイスに自動的にインストールされます。インストールされたプロビジョニングプロファイルは、「設定」>「一般」>「プロファイル」のそのデバイスで見ることができます。

.mobileprovision ファイルをユーザに配信して、ユーザに「iTunes」アプリケーションアイコンにドラッグしてもらってもかまいません。「iTunes」によって、上に定義されている適切な場所にファイルが自動的にコピーされます。

iPhone 構成ユーティリティを使用してプロビジョニングプロファイルをインストールする

「iPhone 構成ユーティリティ」を使用して、接続されているデバイスにプロビジョニングプロファイルをインストールできます。以下の手順に従ってください：

1. 「iPhone 構成ユーティリティ」で、「ファイル」>「ライブラリに追加」と選択してから、インストールしたいプロビジョニングプロファイルを選択します。

   プロファイルが「iPhone 構成ユーティリティ」に追加されたら、「ライブラリ」の「プロビジョニングプロファイル」カテゴリを選択することで見ることができます。

2. 「接続済みデバイス」リストでデバイスを選択します。
3. 「プロビジョニングプロファイル」タブをクリックします。
4. リスト内でプロビジョニングプロファイルを選択して、その「インストール」ボタンをクリックします。

iTunes を使用してアプリケーションをインストールする

ユーザは「iTunes」を使ってアプリケーションをデバイスにインストールします。アプリケーションをセキュリティ保護された状態でユーザに配信してから、以下の手順でインストールしてもらいます：

1. 「iTunes」で、「ファイル」>「ライブラリに追加」と選択し、配信済みのアプリケーション（.app）を選択します。

   .app ファイルを「iTunes」アプリケーションアイコンにドラッグすることもできます。

2. デバイスをコンピュータに接続してから、「iTunes」の「デバイス」リストで選択します。
3. 「アプリケーション」タブをクリックしてから、リストでアプリケーションを選択します。

4 「適用」をクリックすると、アプリケーションとすべての配信プロビジョニングプロファイル（64 ページの「iTunes を使用してプロビジョニングプロファイルをインストールする」の説明で指定されているフォルダにあります）がインストールされます。

iPhone 構成ユーティリティを使用してアプリケーションをインストールする

「iPhone 構成ユーティリティ」を使用して、接続されているデバイスにアプリケーションをインストールできます。以下の手順に従ってください：

1 「iPhone 構成ユーティリティ」で、「ファイル」＞「ライブラリに追加」と選択してから、インストールしたいアプリケーションを選択します。

   アプリケーションが「iPhone 構成ユーティリティ」に追加されたら、「ライブラリ」の「アプリケーション」カテゴリを選択することで見ることができます。

2 「接続済みデバイス」リストでデバイスを選択します。

3 「アプリケーション」タブをクリックします。

4 リスト内でアプリケーションを選択して、その「インストール」ボタンをクリックします。

エンタープライズアプリケーションを使用する

アップルによって署名されていないアプリケーションをユーザが実行すると、使用することを承認している配信プロビジョニングプロファイルがデバイスによって検索されます。プロファイルが見つからない場合は、アプリケーションは開きません。

エンタープライズアプリケーションを無効にする

企業内アプリケーションを無効にする必要がある場合は、配信プロビジョニングプロファイルの署名に使用する固有名を無効にすることで、アプリケーションを無効にすることができます。アプリケーションはそれ以降はインストールできなくなり、すでにインストールされている場合は開かなくなります。

その他の参考資料

アプリケーションとプロビジョニングプロファイルの作成方法について詳しくは、以下を参照してください：

- http://developer.apple.com/jp/iphone/ の「iPhone Dev Center」

Cisco VPN サーバの構成

A

付録

iPhone、iPod touch、および iPad を使用できるように Cisco VPN サーバを構成するときは、以下のガイドラインに従ってください。

対応している Cisco プラットフォーム

iPhone OS は、7.2.x ソフトウェア以降で構成された Cisco ASA 5500 Security Appliances および PIX Firewall に対応しています。最新の 8.0.x ソフトウェアリリース以降をお勧めします。iPhone OS は ISO バージョン 12.4（15）T 以降の Cisco IOS VPN ルーターにも対応しています。VPN 3000 シリーズコンセントレータは iPhone VPN 機能に対応していません。

認証方法

iPhone OS は、以下の認証方法に対応しています：

- 事前共有キーによる IPsec 認証と xauth によるユーザ認証
- クライアント証明書およびサーバ証明書による IPsec 認証と xauth による任意のユーザ認証
- サーバが証明書を提示しクライアントが事前共有キーを提示するハイブリッド認証による IPsec 認証。xauth によるユーザ認証が必要です。
- ユーザ認証では xauth が使用されます。次の認証方法に対応しています：
  - ユーザ名とパスワード
  - RSA SecurID
  - CryptoCard

認証グループ

Cisco Unity プロトコルでは、認証およびその他のパラメータが共通するユーザをまとめるために、認証グループが使用されます。iPhone OS デバイスユーザ用の認証グループを作成することをお勧めします。事前共有キーまたはハイブリッド認証を使用する場合は、デバイス上でグループ名を構成し、グループのパスワードとしてグループの共有シークレット（事前共有キー）を指定する必要があります。

証明書認証を使用する場合は、共有シークレットは使用されず、証明書に含まれるフィールドに基づいてユーザのグループが判別されます。Cisco サーバの設定を使用して、証明書のフィールドをユーザグループにマッピングできます。

証明書

証明書を設定およびインストールするときは、以下の点を確認してください：

- サーバの固有名証明書では、サブジェクト代替名（SubjectAltName）フィールドに、サーバの DNS 名と IP アドレスまたはそのいずれかを指定する必要があります。デバイスでは、この情報によって、証明書がサーバに属しているかどうかが確認されます。SubjectAltName をより柔軟に指定するために、ワイルドカード文字を使用して、セグメント単位で一致させることもできます（例：vpn.*.mycompany.com）。SubjectAltName を指定しない場合は、コモンネームフィールドに DNS 名を指定できます。
- サーバの証明書に署名した CA の証明書をデバイスにインストールする必要があります。CA の証明書がルート証明書でない場合は、信頼チェーンの残りの証明書をインストールして、証明書が信頼されるようにする必要があります。
- クライアント証明書を使用する場合は、クライアントの証明書に署名した信頼された CA 証明書が VPN サーバにインストールされていることを確認します。
- 証明書および認証局（CA）が有効である必要があります（有効期限が切れていないなど）。
- サーバによる証明書チェーンの送信には対応していません。そのため、この機能は無効にする必要があります。
- 証明書による認証を使用する場合は、クライアント証明書に含まれるフィールドに基づいてユーザのグループを識別するようにサーバを設定する必要があります。68 ページの「認証グループ」を参照してください。

IPSec の設定

以下の IPSec 設定を使用してください：

- モード： トンネルモード
- IKE モード： 事前共有キーおよびハイブリッド認証の場合はアグレッシブモード、証明書認証の場合はメインモード
- 暗号化アルゴリズム： 3DES、AES-128、AES-256
- 認証アルゴリズム： HMAC-MD5、HMAC-SHA1
- Diffie Hellman グループ： 事前共有キーおよびハイブリッド認証の場合は、グループ 2 にする必要があります。証明書認証の場合、3DES および AES-128 ではグループ 2 を使用します。AES-256 ではグループ 2 または 5 を使用します。
- PFS（Perfect Forward Secrecy）： PFS を使用する場合、IKE フェーズ 2 では、Diffie-Hellman グループを IKE フェーズ 1 と同じにする必要があります。
- モード構成： 有効にする必要があります。
- DPD（Dead Peer Detection）： 推奨されます。
- 標準 NAT トラバーサル： 対応しており、必要に応じて有効にできます。（IPSec over TCP には対応していません。）
- 負荷分散： 対応しており、必要に応じて有効にできます。
- フェーズ 1 のキー更新： 現時点では対応していません。サーバでのキー更新時間をおよそ 1 時間に設定することをお勧めします。
- ASA アドレスマスク：すべてのデバイスのアドレスプールのマスクが設定されていないか、または 255.255.255.255 に設定されていることを確認してください。 例：

  ```
  asa(config-webvpn)# ip local pool vpn_users 10.0.0.1-10.0.0.254 mask
     255.255.255.255.
  ```

  推奨されたアドレスマスクを使用すると、VPN 構成が想定するルーティングの一部が無視される場合があります。この問題を回避するには、必要なルーティングがルーティングテーブルにすべて含まれていて、サブネットアドレスにアクセスできることを確認してから、配備するようにしてください。

その他の対応機能

iPhone、iPod touch、および iPad は、以下の機能に対応しています：

- アプリケーションバージョン： クライアントソフトウェアのバージョンがサーバに送信されます。これによりサーバは、デバイスのソフトウェアバージョンに基づいて接続を許可または拒否できます。
- バナー： サーバでバナーが構成されている場合は、デバイスにバナーが表示され、ユーザはそれを受け入れるか接続を解除する必要があります。
- スプリット・トンネル： スプリット・トンネリングを利用できます。
- スプリット DNS： スプリット DNS を利用できます。
- デフォルトドメイン： デフォルトドメインを利用できます。

構成プロファイルのフォーマット

B 付録

この付録では、独自のツールを作成したい管理者のために、mobileconfig ファイルのフォーマットについて説明します。

ここでは、アップルの XML DTD および一般的なプロパティリストのフォーマットに精通していることを前提として説明をします。アップルの一般的な plist フォーマットについては、www.apple.com/DTDs/PropertyList-1.0.dtd を参照してください。まず始めに「iPhone 構成ユーティリティ」を使って、この付録の情報を基に変更できるスケルトンファイルを作成してください。

この付録では、ペイロードおよびプロファイルという用語を使用します。プロファイルとは、iPhone、iPod touch、または iPad に特定（単一または複数）の設定を構成するファイル全体のことです。ペイロードとは、プロファイルファイルの個々の構成要素のことです。

ルートレベル

ルートレベルでは、構成ファイルは以下のキー／値ペアを含むディクショナリになります：

キー	値
PayloadVersion	数値、必須。構成プロファイルファイル全体のバージョンです。このバージョン番号は、個々のペイロードではなく、プロファイル全体のフォーマットを示します。
PayloadUUID	文字列、必須。これは通常、人工的に生成された一意の識別文字列です。この文字列は、内容に意味はありませんが、全体で一意である必要があります。Mac OS X では、/usr/bin/uuidgen を使って UUID を生成できます。
PayloadType	文字列、必須。現在のところ、このキーに有効な値は「Configuration」のみです。
PayloadOrganization	文字列、オプション。この値は、プロファイルを発行した組織を示し、ユーザに表示されます。
PayloadIdentifier	文字列、必須。この値は慣例的に、プロファイルを一意に表すドット区切りの文字列です（例：com.myCorp.iPhone.mailSettings、edu.myCollege.students.vpn）。この文字列によってプロファイルが区別されます。プロファイルのインストール時に、同じ識別子を持つ別のプロファイルがあった場合は、追加されるのではなく上書きされます。

キー	値
PayloadDisplayName	文字列、必須。この値は、プロファイルを説明する非常に短い文字列で、ユーザに表示されます（例：VPN 設定）。一意である必要はありません。
PayloadDescription	文字列、オプション。この値は、自由形式の説明テキストで、プロファイル全体の「詳細」画面でユーザに表示されます。この文字列は、インストールすべきかどうかをユーザが判断できるように、プロファイルの内容を明確に示すものにしてください。
PayloadContent	配列、オプション。この値は、プロファイルの実際の内容です。省略した場合は、プロファイル全体が機能を持たなくなります。
PayloadRemovalDisallowed	ブール値、オプション。デフォルトは「No」です。設定した場合、ユーザはプロファイルを削除できなくなります。これが設定されているプロファイルは、プロファイル識別子が一致し、同じ機関によって署名されている場合のみ、USB または Web ／メールを介してアップデートできます。削除用パスワードが指定されている場合は、そのパスワードを指定することでプロファイルを削除できます。 プロファイルが署名済みで暗号化されている場合、プロファイルを変更することはできません。さらに、この設定はデバイス上にも表示されるため、このロッキングビットが目につく状態にあっても問題ありません。

ペイロードの内容

PayloadContent 配列はディクショナリの配列で、各ディクショナリはプロファイルの個々のペイロードを示します。機能を持つプロファイルでは、この配列に 1 つ以上のエントリーが含まれます。この配列内の各ディクショナリには、ペイロードのタイプに関係なく、共通のプロパティがいくつかあります。それ以外のプロパティは、各ペイロードタイプに専用であり一意です。

キー	値
PayloadVersion	数値、必須。個々のペイロードのバージョンです。1 つのプロファイルに異なるバージョン番号のペイロードを含めることができます。たとえば、将来のある時点で、「メール」のバージョン番号はそのままにして、VPN のバージョンを上げることができます。
PayloadUUID	文字列、必須。これは通常、人工的に生成された一意の識別文字列です。この文字列は、内容に意味はありませんが、全体で一意である必要があります。
PayloadType	文字列、必須。このキー／値ペアは、プロファイル内での個々のペイロードのタイプを示します。
PayloadOrganization	文字列、オプション。この値は、プロファイルを発行した組織を示し、ユーザに表示されます。ルートレベルの PayloadOrganization と同じにすることも、別の文字列にすることもできます。
PayloadIdentifier	文字列、必須。この値は慣例的に、ペイロードを一意に表すドット区切りの文字列です。通常は、ルートの PayloadIdentifier にサブ識別子を追加して、特定のペイロードを表します。
PayloadDisplayName	文字列、必須。この値は、プロファイルを説明する非常に短い文字列で、ユーザに表示されます（例：VPN 設定）。一意である必要はありません。
PayloadDescription	文字列、オプション。この値は、自由形式の説明テキストで、このペイロードの「詳細」画面に表示されます。

プロファイル削除用パスワードペイロード

削除用パスワードペイロードであることは、PayloadType 値 com.apple.profileRemovalPassword によって示されます。目的は、ユーザがデバイスから構成プロファイルを削除するためのパスワードをエンコードすることです。このペイロードが指定されていて、パスワード値が設定されている場合は、ユーザがプロファイルの「削除」ボタンをタップしたときにデバイスでパスワードの入力を求められます。このペイロードはプロファイルの残りの部分と共に暗号化されます。

キー	値
RemovalPassword	文字列、オプション。プロファイルの削除用パスワードを指定します。

パスコード・ポリシー・ペイロード

パスコード・ポリシー・ペイロードであることは、PayloadType 値 com.apple.mobiledevice.passwordpolicy によって示されます。このペイロードタイプが含まれる場合は、デバイスでユーザに英数字パスコード入力画面が表示され、特定の長さの複雑なパスコードの入力を要求できます。

すべてのペイロードに共通の設定以外に、このペイロードでは以下の設定を定義できます：

キー	値
allowSimple	ブール値、オプション。デフォルトは「YES」です。単純なパスコードを許可するかどうかを指定します。単純なパスコードとは、文字の繰り返しや昇順／降順の文字列（123、CBA など）を含むパスコードのことです。この値を「NO」に設定すると、minComplexChars を「1」に設定するのと同じ意味になります。
forcePIN	ブール値、オプション。デフォルトは「NO」です。ユーザに PIN の設定を強制するかどうかを指定します。この値だけを設定し、ほかの値を設定しない場合は、ユーザにパスコードの入力が強制されますが、長さや複雑性の制限はなくなります。
maxFailedAttempts	数値、オプション。デフォルトは「11」です。指定可能な範囲は 2 ～ 11 です。デバイスのロック画面でパスコードの入力を失敗できる回数を指定します。この回数を超えると、デバイスがロックされます。この場合、ロックを解除するにはそのデバイスが認証された「iTunes」に接続する必要があります。
maxInactivity	数値、オプション。デフォルトは「Infinity」です。デバイスの待機状態（ユーザがロック解除する必要のない状態）が続いて自動的にロックされるまでの分数を指定します。この制限に達すると、デバイスがロックされてパスコードの入力が必要になります。
maxPINAgeInDays	数値、オプション。デフォルトは「Infinity」です。同じパスコードを使用できる日数を指定します。この日数が過ぎると、デバイスをロック解除するためにパスコードの変更が必要になります。
minComplexChars	数値、オプション。デフォルトは「0」です。パスコードに含める必要のある複合文字の最小数を指定します。複合文字とは、数字または文字以外の文字（&、%、$、# など）のことです。

キー	値
minLength	数値、オプション。デフォルトは「0」です。パスコードの最小限の長さを指定します。このパラメータと、同様にオプションである minComplexChars 引数との間に依存関係はありません。
requireAlphanumeric	ブール値、オプション。デフォルトは「NO」です。アルファベット（a、b、c、d など）を含める必要があるか、または数字だけを許可するかを指定します。
pinHistory	数値、オプション。ユーザがパスコードを変更するときは、履歴の最後の N 個のエントリー内で一意である必要があります。最小値は 1 で、最大値は 50 です。
manualFetchingWhenRoaming	ブール値、オプション。設定した場合、ローミング時にすべてのプッシュ操作が無効になります。ユーザは新しいデータを手動でフェッチする必要があります。
maxGracePeriod	数値、オプション。パスコードを入力せずに電話のロックを解除するための、最大の猶予期間（分単位）。デフォルトは 0（猶予期間なし）で、即座にパスコードが必要になります。

メールペイロード

メールペイロードであることは、PayloadType 値 com.apple.mail.managed によって示されます。このペイロードでは、デバイス上にメールアカウントが作成されます。すべてのペイロードに共通の設定以外に、このペイロードでは以下の設定を定義できます：

キー	値
EmailAccountDescription	文字列、オプション。メールアカウントの説明です。「メール」および「設定」アプリケーションでユーザに表示されます。
EmailAccountName	文字列、オプション。アカウントのユーザのフルネームです。このユーザ名は、送信メッセージなどで使用されます。
EmailAccountType	文字列、必須。指定可能な値は「EmailTypePOP」と「EmailTypeIMAP」です。アカウントに使用するプロトコルを定義します。
EmailAddress	文字列、必須。アカウントの完全なメールアドレスを指定します。ペイロードで指定しない場合は、デバイスでプロファイルのインストール時にこの文字列の入力が求められます。
IncomingMailServerAuthentication	文字列、必須。受信メールの認証方法を指定します。指定可能な値は「EmailAuthPassword」と「EmailAuthNone」です。
IncomingMailServerHostName	文字列、必須。受信メールサーバのホスト名（または IP アドレス）を指定します。
IncomingMailServerPortNumber	数値、オプション。受信メールサーバのポート番号を指定します。ポート番号を指定しない場合は、指定されたプロトコルのデフォルトのポートが使用されます。
IncomingMailServerUseSSL	ブール値、オプション。デフォルトは「Yes」です。受信メールサーバで認証に SSL を使用するかどうかを指定します。
IncomingMailServerUsername	文字列、必須。メールアカウントのユーザ名を指定します。通常は、メールアドレスの @ より前の文字列になります。ペイロードで指定しない場合、受信メールで認証を行うようにアカウントが設定されているときは、デバイスでプロファイルのインストール時にこの文字列の入力が求められます。

キー	値
IncomingPassword	文字列、オプション。受信メールサーバのパスワード。暗号化されたプロファイルのみで使用します。
OutgoingPassword	文字列、オプション。送信メールサーバのパスワード。暗号化されたプロファイルのみで使用します。
OutgoingPasswwordSameAsIncomingPassword	ブール値、オプション。設定した場合、ユーザは 1 回だけパスワードの入力を求められ、それが送信メールと受信メールの両方で使用されます。
OutgoingMailServerAuthentication	文字列、必須。送信メールの認証方法を指定します。指定可能な値は「EmailAuthPassword」と「EmailAuthNone」です。
OutgoingMailServerHostName	文字列、必須。送信メールサーバのホスト名（または IP アドレス）を指定します。
OutgoingMailServerPortNumber	数値、オプション。送信メールサーバのポート番号を指定します。ポート番号を指定しない場合は、ポート 25、587、465 がこの順番で使用されます。
OutgoingMailServerUseSSL	ブール値、オプション。デフォルトは「Yes」です。送信メールサーバで認証に SSL を使用するかどうかを指定します。
OutgoingMailServerUsername	文字列、必須。メールアカウントのユーザ名を指定します。通常は、メールアドレスの @ より前の文字列になります。ペイロードで指定しない場合、送信メールで認証を行うようにアカウントが設定されているときは、デバイスでプロファイルのインストール時にこの文字列の入力が求められます。

Web クリップペイロード

Web クリップペイロードであることは、PayloadType 値 com.apple.webClip.managed によって示されます。すべてのペイロードに共通の設定以外に、このペイロードでは以下の設定を定義できます：

キー	値
URL	文字列、必須。クリックすると Web クリップが開く URL。URL は HTTP または HTTPS で始まる必要があります。それ以外の場合は機能しません。
Label	文字列、必須。ホーム画面に表示される Web クリップの名前。
Icon	データ、オプション。ホーム画面に表示される PNG アイコン。サイズは 59 × 60 ピクセルにする必要があります。指定しない場合は、白い四角が表示されます。
IsRemovable	ブール値、オプション。「No」の場合、ユーザが Web クリップを削除することはできませんが、プロファイルが削除された場合は削除されます。

制限ペイロード

制限ペイロードであることは、PayloadType 値 com.apple.applicationaccess によって示されます。すべてのペイロードに共通の設定以外に、このペイロードでは以下の設定を定義できます：

キー	値
allowAppInstallation	ブール値、オプション。偽のときは、App Store は無効になり、アイコンがホーム画面から削除されます。ユーザはアプリケーションをインストールまたはアップデートできません。
allowCamera	ブール値、オプション。偽のときは、カメラは完全に無効になり、アイコンがホーム画面から削除されます。ユーザは写真を撮ることはできません。
allowExplicitContent	ブール値、オプション。偽のときは、iTunes Store から購入した露骨な内容の音楽やビデオが隠されます。露骨な内容は、iTunes Store から販売されるときに、レコード会社などのコンテンツプロバイダによって露骨な内容として指定されています。
allowScreenShot	ブール値、オプション。偽のときは、ユーザはディスプレイのスクリーンショットを保存できません。
allowYouTube	ブール値、オプション。偽のときは、「YouTube」アプリケーションは無効になり、アイコンがホーム画面から削除されます。
allowiTunes	ブール値、オプション。偽のときは、iTunes Music Store は無効になり、アイコンがホーム画面から削除されます。ユーザはコンテンツをプレビュー、購入、およびダウンロードできません。
allowSafari	ブール値、オプション。偽のときは、Safari Web ブラウザアプリケーションは無効になり、アイコンがホーム画面から削除されます。ユーザが Web クリップを開くこともできなくなります。

LDAP ペイロード

LDAP ペイロードであることは、PayloadType 値 com.apple.ldap.account によって示されます。LDAP Account から LDAPSearchSettings まで 1 対多の関係があります。LDAP をツリーとして考えます。各 SearchSettings オブジェクトは検索を始めるツリー内のノードと、検索対象の範囲（ノード、ノードと 1 つのレベルの子、ノードとすべてのレベルの子）を表します。すべてのペイロードに共通の設定以外に、このペイロードでは以下の設定を定義できます：

キー	値
LDAPAccountDescription	文字列、オプション。アカウントの説明。
LDAPAccountHostName	文字列、必須。ホスト。
LDAPAccountUseSSL	ブール値、必須。SSL を使用するかどうか。
LDAPAccountUserName	文字列、オプション。ユーザ名。
LDAPAccountPassword	文字列、オプション。暗号化されたプロファイルのみで使用します。
LDAPSearchSettings	最上位のコンテナオブジェクト。1 つのアカウントに複数設定できます。有効にするには、アカウントに 1 つ以上設定する必要があります。
LDAPSearchSettingDescription	文字列、オプション。この検索設定の説明。

キー	値
LDAPSearchSettingSearchBase	文字列、必須。概念的には、「ou=people,o=example corp」で検索を始めるためのノードへのパス
LDAPSearchSettingScope	文字列、必須。検索で使用する再帰を定義します。 以下の 3 つの値のいずれかにすることができます： LDAPSearchSettingScopeBase：SearchBase によって指定された即値ノード。 LDAPSearchSettingScopeOneLevel：ノードとその直接の子。 LDAPSearchSettingScopeSubtree：ノードと、深さを問わずすべての子。

CalDAV ペイロード

CalDAV ペイロードであることは、PayloadType 値 com.apple.caldav.account によって示されます。すべてのペイロードに共通の設定以外に、このペイロードでは以下の設定を定義できます：

キー	値
CalDAVAccountDescription	文字列、オプション。アカウントの説明。
CalDAVHostName	文字列、必須。サーバアドレス
CalDAVUsername	文字列、必須。ユーザのログイン名。
CalDAVPassword	文字列、オプション。ユーザのパスワード
CalDAVUseSSL	ブール値、必須。SSL を使用するかどうか。
CalDAVPort	数値、オプション。サーバに接続するポート。
CalDAVPrincipalURL	文字列、オプション。ユーザのカレンダーへのベース URL。

カレンダーの照会ペイロード

CalSub ペイロードであることは、PayloadType 値 com.apple.subscribedcalendar.account によって示されます。すべてのペイロードに共通の設定以外に、このペイロードでは以下の設定を定義できます：

キー	値
SubCalAccountDescription	文字列、オプション。アカウントの説明。
SubCalAccountHostName	文字列、必須。サーバアドレス。
SubCalAccountUsername	文字列、オプション。ユーザのログイン名。
SubCalAccountPassword	文字列、オプション。ユーザのパスワード。
SubCalAccountUseSSL	ブール値、必須。SSL を使用するかどうか。

SCEP ペイロード

SCEP（Simple Certificate Enrollment Protocol）ペイロードであることは、PayloadType 値 com.apple.encrypted-profile-service によって示されます。すべてのペイロードに共通の設定以外に、このペイロードでは以下の設定を定義できます：

キー	値
URL	文字列、必須。
Name	文字列、オプション。SCEP サーバによって解釈される文字列。たとえば、example.org のようなドメイン名の場合があります。認証局が複数の CA 証明書を持っている場合は、このフィールドを使用して必要な CA 証明書を識別できます。
Subject	配列、オプション。OID および値の配列として表される X.500 名の表現。たとえば、「/C=US/O=Apple Inc./CN=foo/1.2.5.3=bar」です。これは以下のように変換されます： [[[“C“, “US“]], [[“O“, “Apple Inc.“]], ..., [[“1.2.5.3“, “bar“]]] OID は、ドット付きの数字として、C、L、ST、O、OU、CN（国、地域、州、組織、組織単位、コモンネーム）のショートカットと共に指定できます。
Challenge	文字列、オプション。事前共有シークレット。
Keysize	数値、オプション。ビット単位のキーサイズで、1024 または 2048 のいずれか。
Key Type	文字列、オプション。現在は常に「RSA」です。
Key Usage	数値、オプション。キーの用途を示すビットマスク。1 は署名、4 は暗号化、5 は署名と暗号化の両方です。Windows CA など一部の CA は暗号化のみまたは署名のみをサポートし、両方を同時にはサポートしません。

SubjectAltName ディクショナリキー

SCEP ペイロードに SubjectAltName ディクショナリを指定して、CA が証明書を発行するために必要な値を記述することもできます。キーごとに、1 つの文字列または文字列の配列を指定できます。指定する値は使用する CA によって異なりますが、DNS 名、URL、またはメール値を指定します。85 ページの「フェーズ 3 - SCEP 仕様によるサーバ応答のサンプル」の例を参照してください。

GetCACaps ディクショナリキー

GetCACaps キーでディクショナリを追加したデバイスは、指定されている文字列を CA の能力に関する信頼できる情報ソースとして使用します。追加していないデバイスは、CA に GetCACaps を照会し、返された内容を使用します。CA が応答しない場合は、デフォルトの動作として GET 3DES および SHA-1 要求を行います。

APN ペイロード

APN（アクセスポイント名）ペイロードであることは、PayloadType 値 com.apple.apn.managed によって示されます。すべてのペイロードに共通の設定以外に、このペイロードでは以下の設定を定義できます：

キー	値
DefaultsData	ディクショナリ、必須。このディクショナリでは、2 つのキー／値ペアを指定します。
DefaultsDomainName	文字列、必須。指定可能な値は「com.apple.managedCarrier」のみです。
apns	配列、必須。この配列には任意の数のディクショナリを含めることができ、各ディクショナリで以下のキー／値ペアによって APN 構成を指定します。
apn	文字列、必須。この文字列では、アクセスポイント名を指定します。
username	文字列、必須。この文字列では、この APN のユーザ名を指定します。指定しない場合は、デバイスでプロファイルのインストール時に入力を求められます。
password	データ、オプション。このデータでは、この APN のユーザのパスワードを指定します。解読されないようにエンコードされます。ペイロードで指定しない場合は、デバイスでプロファイルのインストール時に入力を求められます。
proxy	文字列、オプション。APN プロキシの IP アドレスまたは URL。
proxyPort	数値、オプション。APN プロキシのポート番号。

Exchange ペイロード

Exchange ペイロードであることは、PayloadType 値 com.apple.eas.account によって示されます。このペイロードでは、デバイス上に Microsoft Exchange アカウントが作成されます。すべてのペイロードに共通の設定以外に、このペイロードでは以下の設定を定義できます：

キー	値
EmailAddress	文字列、必須。ペイロードで指定しない場合は、デバイスでプロファイルのインストール時にこの文字列の入力が求められます。アカウントの完全なメールアドレスを指定します。
Host	文字列、必須。Exchange サーバのホスト名（または IP アドレス）を指定します。
SSL	ブール値、オプション。デフォルトは「YES」です。Exchange サーバで認証に SSL を使用するかどうかを指定します。
UserName	文字列、必須。この文字列では、この Exchange アカウントのユーザ名を指定します。指定しない場合は、デバイスでプロファイルのインストール時に入力を求められます。
Password	文字列、オプション。アカウントのパスワード。暗号化されたプロファイルのみで使用します。
Certificate	オプション。証明書による認証が可能なアカウントの場合は、NSData blob フォーマットの .p12 固有名証明書。

キー	値
CertificateName	文字列、オプション。証明書の名前または説明を指定します。
CertificatePassword	オプション。p12 固有名証明書に必要なパスワード。暗号化されたプロファイルのみで使用します。

VPN ペイロード

VPN ペイロードであることは、PayloadType 値 com.apple.vpn.managed によって示されます。すべてのペイロードタイプに共通の設定以外に、VPN ペイロードでは以下のキーを定義できます。

キー	値
UserDefinedName	文字列。デバイスに表示される VPN 接続の説明です。
OverridePrimary	ブール値。すべてのトラフィックを VPN インターフェイス経由で送信するかどうかを指定します。「true」に設定した場合は、すべてのネットワークトラフィックが VPN 経由で送信されます。
VPNType	文字列。このタイプの VPN 接続のペイロードで利用可能な設定を指定します。指定可能な値は「L2TP」、「PPTP」、「IPSec」の 3 つで、それぞれ L2TP、PPTP、Cisco IPSec に対応します。

最上位の「PPP」キーと「IPSec」キーにそれぞれディクショナリを定義できます。以下では、これら 2 つのディクショナリ内のキーについての説明と、そのキーが使用される VPNType の値を示します。

PPP ディクショナリキー

以下の要素は PPP タイプの VPN ペイロードで使用されます。

キー	値
AuthName	文字列。VPN アカウントのユーザ名です。L2TP および PPTP で使用されます。
AuthPassword	文字列、オプション。TokenCard が「false」の場合にのみ表示されます。L2TP および PPTP で使用されます。
TokenCard	ブール値。接続に RSA SecurID などのトークンカードを使用するかどうかを指定します。L2TP で使用されます。
CommRemoteAddress	文字列。VPN サーバの IP アドレスまたはホスト名です。L2TP および PPTP で使用されます。
AuthEAPPlugins	配列。RSA SecurID を使用する場合にのみ表示されます。使用する場合、エントリーは 1 つで、値は文字列「EAP-RSA」になります。L2TP および PPTP で使用されます。
AuthProtocol	配列。RSA SecurID を使用する場合にのみ表示されます。使用する場合、エントリーは 1 つで、値は文字列「EAP」になります。L2TP および PPTP で使用されます。
CCPMPPE40Enabled	ブール値。CCPEnabled の説明を参照してください。PPTP で使用されます。

キー	値
CCPMPPE128Enabled	ブール値。CCPEnabled の説明を参照してください。PPTP で使用されます。
CCPEnabled	ブール値。接続の暗号化を有効にします。このキーと CCPMPPE40Enabled が「true」の場合は、自動の暗号化レベルに設定されます。このキーと CCPMPPE128Enabled が「true」の場合は、最大の暗号化レベルに設定されます。暗号化を使用しない場合は、すべての CCP キーを「true」にしないようにします。PPTP で使用されます。

IPSec ディクショナリキー

以下の要素は IPSec タイプの VPN ペイロードで使用されます。

キー	値
RemoteAddress	文字列。VPN サーバの IP アドレスまたはホスト名です。Cisco IPSec で使用されます。
AuthenticationMethod	文字列。「SharedSecret」または「Certificate」のいずれかを指定します。L2TP および Cisco IPSec で使用されます。
XAuthName	文字列。VPN アカウントのユーザ名です。Cisco IPSec で使用されます。
XAuthEnabled	整数。XAUTH を有効にする場合は「1」、無効にする場合は「0」を指定します。Cisco IPSec で使用されます。
LocalIdentifier	文字列。AuthenticationMethod が「SharedSecret」の場合にのみ表示されます。使用するグループの名前を指定します。ハイブリッド認証を使用する場合は、この文字列の末尾に「[hybrid]」を付ける必要があります。Cisco IPSec で使用されます。
LocalIdentifierType	文字列。AuthenticationMethod が「SharedSecret」の場合にのみ表示されます。値は「KeyID」です。L2TP および Cisco IPSec で使用されます。
SharedSecret	データ。この VPN アカウントの共有シークレットです。AuthenticationMethod が「SharedSecret」の場合にのみ表示されます。L2TP および Cisco IPSec で使用されます。
PayloadCertificateUUID	文字列。アカウント資格情報に使用する証明書の UUID です。AuthenticationMethod が「Certificate」の場合にのみ表示されます。Cisco IPSec で使用されます。
PromptForVPNPIN	ブール値。接続時に PIN の入力を求めるかどうかを指定します。Cisco IPSec で使用されます。

Wi-Fi ペイロード

Wi-Fi ペイロードであることは、PayloadType 値 com.apple.wifi.managed によって示されます。ここでは、PayloadVersion 値バージョン 0 について説明します。すべてのペイロードタイプに共通の設定以外に、このペイロードでは以下のキーを定義できます。

キー	値
SSID_STR	文字列。使用する Wi-Fi ネットワークの SSID です。
HIDDEN_NETWORK	ブール値。デバイスでは、ネットワークを区別するために、SSID 以外にブロードキャストのタイプや暗号化のタイプなどの情報も使用されます。デフォルトでは、構成されたすべてのネットワークが公開されているものまたはブロードキャストであるとみなされます。非公開のネットワークを指定するには、HIDDEN_NETWORK キーのブール値を指定する必要があります。
EncryptionType	文字列。EncryptionType に指定可能な値は「WEP」、「WPA」、または「Any」です。「WPA」は、WPA および WPA2 に対応し、両方の暗号化タイプに該当します。これらの値は必ず、ネットワーク・アクセス・ポイントの機能と正確に一致させてください。暗号化タイプが分からない場合、またはすべての暗号化タイプに該当させたい場合は、「Any」を使用します。
Password	文字列、オプション。パスワードを指定しなくても、既知のネットワークの一覧にネットワークが追加されます。ユーザがネットワークに接続するときに、パスワードの入力を求められます。

802.1X エンタープライズネットワークを使用する場合は、EAP クライアント構成ディクショナリを指定する必要があります。

EAPClientConfiguration ディクショナリ

標準的な暗号化タイプ以外に、EAPClientConfiguration キーを使用して特定のネットワークのエンタープライズプロファイルを指定できます。このキーを使用する場合、値は以下のキーを含むディクショナリになります。

キー	値
UserName	文字列、オプション。正確なユーザ名が分からない場合は、読み込まれた構成にこのプロパティは表示されません。ユーザは認証時に自分でこの情報を入力できます。
AcceptEAPTypes	整数値の配列。次のタイプの EAP が受け入れられます： 13 = TLS 17 = LEAP 21 = TTLS 25 = PEAP 43 = EAP-FAST

キー	値
PayloadCertificateAnchorUUID	文字列の配列、オプション。この認証で信頼される証明書を識別します。各エントリーに証明書ペイロードの UUID が含まれている必要があります。リストされた証明書が信頼されているかどうかをデバイスがユーザに確認しないようにするには、このキーを使用します。 このプロパティを指定した場合は、TLSAllowTrustExceptions を「true」に設定した場合を除いて、動的な信頼（証明書ダイアログ）が無効になります。
TLSTrustedServerNames	文字列値の配列、オプション。受け入れるサーバ証明書のコモンネームのリストです。ワイルドカードを使用して名前を指定することもできます（例：wpa.*.example.com）。このリストにない証明書をサーバが提示した場合、そのサーバは信頼されません。 このプロパティを単独で使用するか TLSTrustedCertificates と一緒に使用して、特定のネットワークで信頼される証明書のリストをきちんと作成すれば、証明書を動的に信頼してもらう必要がなくなります。 このプロパティを指定した場合は、TLSAllowTrustExceptions を「true」に設定した場合を除いて、動的な信頼（証明書ダイアログ）が無効になります。
TLSAllowTrustExceptions	ブール値、オプション。ユーザが信頼性を動的に決定するのを許可または禁止します。動的な信頼とは、証明書が信頼されていないときに表示される証明書ダイアログのことです。これを「false」に設定すると、証明書があらかじめ信頼されていない限り認証に失敗します。前述の PayloadCertificateAnchorUUID と TLSTrustedNames を参照してください。 このプロパティのデフォルト値は、PayloadCertificateAnchorUUID または TLSTrustedServerNames が指定されていない場合は「true」、指定されている場合は「false」です。
TTLSInnerAuthentication	文字列、オプション。これは、TTLS モジュールで使用される内部認証です。デフォルト値は「MSCHAPv2」です。 指定可能な値は「PAP」、「CHAP」、「MSCHAP」、および「MSCHAPv2」です。
OuterIdentity	文字列、オプション。このキーは、TTLS、PEAP、および EAP-FAST でのみ使用されます。 この設定を使用すると、ユーザが自分の固有名を隠すことができます。ユーザの実際の名前は、暗号化されたトンネル内でのみ表示されます。たとえば、「anonymous」、「anon」、「anon@mycompany.net」などに設定できます。 認証を行っているユーザの名前を攻撃者がクリアテキストで見ることができないため、セキュリティを高めることができます。

EAP-Fast への対応

EAP-FAST モジュールでは、EAPClientConfiguration ディクショナリで以下のプロパティが使用されます。

キー	値
EAPFASTUsePAC	ブール値、オプション。
EAPFASTProvisionPAC	ブール値、オプション。
EAPFASTProvisionPACAnonymously	ブール値、オプション。

これらのキーには、階層的な性質があります。EAPFASTUsePAC を「false」にすると、残りの 2 つのプロパティは無視されます。同様に、EAPFASTProvisionPAC を「false」にすると、EAPFASTProvisionPACAnonymously は無視されます。

EAPFASTUsePAC を「false」にした場合、認証は PEAP または TTLS とほぼ同じように行われます。サーバが毎回、証明書を使用して身元を証明します。

EAPFASTUsePAC を「true」にした場合、既存の PAC があるときはそれが使用されます。現在のところ、デバイスで PAC を取得する方法には、PAC のプロビジョニングを許可する方法しかありません。そのため、EAPFASTProvisionPAC を有効にし、必要に応じて EAPFASTProvisionPACAnonymously を有効にする必要があります。EAPFASTProvisionPACAnonymously にはセキュリティ上の弱点があります。これを使用するとサーバが認証されないため、中間者攻撃を受けやすくなります。

証明書

VPN 構成と同様に、証明書の固有名構成を Wi-Fi 構成に関連付けることができます。これは、セキュリティ保護されたエンタープライズネットワークの資格情報を定義するときに便利です。固有名を関連付けるには、その固有名のペイロードの UUID を PayloadCertificateUUID キーに指定します。

キー	値
PayloadCertificateUUID	文字列。固有名資格情報に使用する証明書ペイロードの UUID です。

サンプルの構成プロファイル

このセクションでは、無線での登録と構成フェーズが記述されているサンプルプロファイルを紹介します。ここで示すのはサンプルであり、実際に必要なものとは異なります。構文を理解するために、この付録ですでに説明した詳細を参照してください。各フェーズの説明は、22 ページの「無線での登録と構成」を参照してください。

フェーズ 1 – サーバ応答のサンプル

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN" "http://
     www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>PayloadContent</key>
    <dict>
        <key>URL</key>
        <string>https://profileserver.example.com/iphone</string>
        <key>DeviceAttributes</key>
        <array>
               <string>UDID</string>
  <string>IMEI</string>
  <string>ICCID</string>
  <string>VERSION</string>
```

```
  <string>PRODUCT</string>
        </array>
    <key>Challenge</key>
     <string> オプションのチャレンジ </string>
     または
     <data>base64-encoded</data>
    </dict>
    <key>PayloadOrganization</key>
    <string>Example Inc.</string>
    <key>PayloadDisplayName</key>
    <string> プロファイルサービス </string>
    <key>PayloadVersion</key>
    <integer>1</integer>
    <key>PayloadUUID</key>
    <string>fdb376e5-b5bb-4d8c-829e-e90865f990c9</string>
    <key>PayloadIdentifier</key>
    <string>com.example.mobileconfig.profile-service</string>
    <key>PayloadDescription</key>
    <string>Example Inc の暗号化されたプロファイルサービスにデバイスを入力します </string>
    <key>PayloadType</key>
     <string> プロファイルサービス </string>
</dict>
</plist>
```

フェーズ 2 - デバイス応答のサンプル

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
     DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>UDID</key>
    <string></string>
    <key>VERSION</key>
    <string>7A182</string>
    <key>MAC_ADDRESS_EN0</key>
    <string>00:00:00:00:00:00</string>
    <key>CHALLENGE</key>
次のいずれか：
    <string> 文字列 </string>
または：
    <data>"base64 エンコードのデータ "</data>
</dict>
</plist>
```

フェーズ 3 - SCEP 仕様によるサーバ応答のサンプル

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple Inc//DTD PLIST 1.0//EN" "http://
     www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
  <dict>
    <key>PayloadVersion</key>
    <integer>1</integer>
    <key>PayloadUUID</key>
    <string> 無視 </string>
    <key>PayloadType</key>
    <string> 構成 </string>
    <key>PayloadIdentifier</key>
    <string> 無視 </string>
    <key>PayloadContent</key>
    <array>
      <dict>
        <key>PayloadContent</key>
        <dict>
          <key>URL</key>
          <string>https://scep.example.com/scep</string>
          <key>Name</key>
          <string>EnrollmentCAInstance</string>
          <key>Subject</key>
          <array>
            <array>
              <array>
                <string>O</string>
                <string>Example, Inc.</string>
              </array>
            </array>
            <array>
              <array>
                <string>CN</string>
                <string> ユーザデバイス証明書 </string>
              </array>
            </array>
          </array>
          <key>Challenge</key>
          <string>...</string>
          <key>Keysize</key>
          <integer>1024</integer>
          <key>Key Type</key>
          <string>RSA</string>
          <key>Key Usage</key>
          <integer>5</integer>
```

```
        </dict>
        <key>PayloadDescription</key>
        <string> デバイス暗号化固有名を入力します </string>
        <key>PayloadUUID</key>
        <string>fd8a6b9e-0fed-406f-9571-8ec98722b713</string>
        <key>PayloadType</key>
        <string>com.apple.security.scep</string>
        <key>PayloadDisplayName</key>
        <string> 暗号化固有名 </string>
        <key>PayloadVersion</key>
        <integer>1</integer>
        <key>PayloadOrganization</key>
        <string>Example, Inc.</string>
        <key>PayloadIdentifier</key>
        <string>com.example.profileservice.scep</string>
      </dict>
    </array>
  </dict>
</plist>
```

フェーズ 4 - デバイス応答のサンプル

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/
     DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
    <key>UDID</key>
    <string></string>
    <key>VERSION</key>
    <string>7A182</string>
    <key>MAC_ADDRESS_EN0</key>
    <string>00:00:00:00:00:00</string>
</dict>
</plist>
```

サンプルスクリプト

付録 C

この付録では、iPhone OS 配備タスクのサンプルスクリプトを紹介します。

このセクションのスクリプトは、実際の要件と構成に合わせて変更する必要があります。

iPhone 構成ユーティリティ用の C# サンプルスクリプト

このサンプルスクリプトは、Windows 用の「iPhone 構成ユーティリティ」を使って構成ファイルを作成する例を示しています。

```
using System;
using Com.Apple.iPCUScripting;

public class TestScript : IScript
  {
  private IApplication _host;

  public TestScript()
     {
     }

  public void main(IApplication inHost)
     {
     _host = inHost;

     string msg = string.Format("# of config profiles : {0}",
     _host.ConfigurationProfiles.Count);
     Console.WriteLine(msg);

     IConfigurationProfile profile = _host.AddConfigurationProfile();
     profile.Name = "Profile Via Script";
     profile.Identifier = "com.example.configviascript";
     profile.Organization = "Example Org";
     profile.Description = "This is a configuration profile created via the
     new scripting feature in iPCU";

     // passcode
     IPasscodePayload passcodePayload = profile.AddPasscodePayload();
     passcodePayload.PasscodeRequired = true;
```

```
passcodePayload.AllowSimple = true;

// restrictions
IRestrictionsPayload restrictionsPayload =
profile.AddRestrictionsPayload();
restrictionsPayload.AllowYouTube = false;

// wi-fi
IWiFiPayload wifiPayload = profile.AddWiFiPayload();
wifiPayload.ServiceSetIdentifier = "Example Wi-Fi";
wifiPayload.EncryptionType = WirelessEncryptionType.WPA;
wifiPayload.Password = "password";

wifiPayload = profile.AddWiFiPayload();
profile.RemoveWiFiPayload(wifiPayload);

// vpn
IVPNPayload vpnPayload = profile.AddVPNPayload();
vpnPayload.ConnectionName = "Example VPN Connection";

vpnPayload = profile.AddVPNPayload();
profile.RemoveVPNPayload(vpnPayload);

// email
IEmailPayload emailPayload = profile.AddEmailPayload();
emailPayload.AccountDescription = "Email Account 1 Via Scripting";

emailPayload = profile.AddEmailPayload();
emailPayload.AccountDescription = "Email Account 2 Via Scripting";

// exchange
IExchangePayload exchangePayload = profile.AddExchangePayload();
exchangePayload.AccountName = "ExchangePayloadAccount";

// ldap
ILDAPPayload ldapPayload = profile.AddLDAPPayload();
ldapPayload.Description = "LDAP Account 1 Via Scripting";

ldapPayload = profile.AddLDAPPayload();
ldapPayload.Description = "LDAP Account 2 Via Scripting";

// webclip
IWebClipPayload wcPayload = profile.AddWebClipPayload();
wcPayload.Label = "Web Clip 1 Via Scripting";

wcPayload = profile.AddWebClipPayload();
wcPayload.Label = "Web Clip 2 Via Scripting";

    }
}
```

iPhone 構成ユーティリティ用のサンプル AppleScript

このサンプルスクリプトは、Mac OS X 用の「iPhone 構成ユーティリティ」を使って構成ファイルを作成する例を示しています。

```
tell application "iPhone Configuration Utility"
  log (count of every configuration profile)
  set theProfile to make new configuration profile with properties {displayed
     name:"Profile Via Script", profile
     identifier:"com.example.configviascript", organization:"Example Org.",
     account description:"This is a configuration profile created via
     AppleScript"}
  tell theProfile
     make new passcode payload with properties {passcode required:true, simple
     value allowed:true}
     make new restrictions payload with properties {YouTube allowed:false}
     make new WiFi payload with properties {service set identifier:"Example
     Wi-Fi", security type:WPA, password:"password"}
     set theWiFiPayload to make new WiFi payload
     delete theWiFiPayload
     make new VPN payload with properties {connection name:"Example VPN
     Connection"}
     set theVPNPayload to make new VPN payload
     delete theVPNPayload
     make new email payload with properties {account description:"Email
     Account 1 Via Scripting"}
     make new email payload with properties {account description:"Email
     Account 2 Via Scripting"}
     make new Exchange ActiveSync payload with properties {account
     name:"ExchangePayloadAccount"}
     make new LDAP payload with properties {account description:"LDAP Account
     1 Via Scripting"}
     make new LDAP payload with properties {account description:"LDAP Account
     2 Via Scripting"}
     make new web clip payload with properties {label:"Web Clip Account 1 Via
     Scripting"}
     make new web clip payload with properties {label:"Web Clip Account 2 Via
     Scripting"}
  end tell
end tell
```